IdentityIQ Reports

Version: 8.3

Revised: April 2022

Copyright and Trademark Notices

Contents

Reports Introduction

> Your level of access determines what information is displayed on each page and tab.

Reports provide an at-a-glance view of the data in IdentityIQ, which helps the organization manage system access and the compliance process. IdentityIQ includes a standard set of core reports in template form. Individual users and organizations can customize and save instances of these templates, and run these reports on a scheduled or ad-hoc basis. Additionally, custom reports can be created to meet the needs of each customer.

IdentityIQ includes a reporting architecture that simplifies the process of creating custom reports. Basic reports can be created quickly through an XML specification. A variety of hooks are available for introducing more complex logic where it is needed to produce the desired report output. The standard report templates that are part of the product are modeled with this same XML specification structure and can serve as helpful examples of how custom reports should be structured.

Report Terminology

IdentityIQ uses these terms for describing how to create custom reports and how to customize report templates:

- **Report Templates**: Out-of-the-box reports provided with the standard IdentityIQ product. These report templates are on the **Reports** tab of the Reports page (under the **Intelligence > Reports** menu). These reports can be run directly, or edited to create customized versions. These reports are also referred to as out-of-the-box reports, standard reports, or standard report templates.
- **Custom Reports**: Customer-specific reports developed by or specifically for a single customer through a custom Task Definition specification. Once they have been saved, these reports are on the **Reports** tab of the Reports page. These reports are also referred to as custom report templates.
- **Customized Report Instances** — User-specific report versions with pre-specified parameters. These reports are on the **My Reports** tab of the Reports page. Instances apply to out-of-the-box reports and custom reports. The terms customized report or instance are also used for these reports.

Report Administration

> Your level of access determines what information is displayed on each page and tab.

IdentityIQ includes a number of standard reports for monitoring and managing compliance and provisioning activities. These reports can be run with or without filter criteria. For example, the Uncorrelated Accounts Report can run with no filters and return the list of uncorrelated accounts for all applications in the system, or you can set filters on the report, to restrict the results to a subset of applications.

The unfiltered, standard version of each report is listed on, and can be run from, the Report page's Reports tab. If you add filters to the standard report, that report configuration is saved as a customized report on the **My Reports** tab.

To access the Reports page, from the Navigation menu bar, go to **Intelligence > Reports**.

For more information see:

My Reports Tab

Reports Tab

Edit Report Page

Scheduled Reports Tab

Report Results Tab

XML Representation of Reports and Instances

Developing Custom Reports

Reports DataSource Example

Report Use

Reports Tab

The Reports tab lists all the available report templates, grouped by category. The out-of-the-box report categories are:

- Access Review and Certification Reports
- Account Group Reports
- Activity Reports
- Administration Reports
- Application Reports
- Configured Resources Reports
- Identity and User Reports
- Lifecycle Manager Reports
- Policy Enforcement Reports
- Risk Reports
- Role Management Reports

Use the **Search by Report Name** field to find the report you want to run. The **Filter searches by** setting in the **gear menu > Global Settings > IdentityIQ Configuration > Miscellaneous** tab, in the **Reporting** section, determines

whether the search will find only reports that *start with* the string you entered, or reports that *contain* the string anywhere in the name.

This tab lists each report name and a brief description of its contents. You can run reports run directly from this page or schedule them to run at some point in the future, either once or on a repeating, scheduled basis. Any report initiated (immediately or scheduled) directly from this page is run with no filters applied. In other words, the report runs for all system objects to which that report applies (all roles, all Identities, all policies, all access reviews, etc.).

To run a report with no filters, right-click and choose **Execute** to run it once immediately or **Schedule** to set it up to run in the future or on a repeating basis.

To edit the report template to add details and filtering criteria, click on the report name, or right-click and choose **Edit**.

To completely remove the report from the system, click **Delete**.

You can also create a new report that saves any filters and other parameters you want to add. Click the report name in the list or right-click the report and choose **Save as New Report**. Both of these options open the Edit Report Page that displays the available filters and parameters for the report.

Edit Report Page

The Edit Report page is where you set details and filters for the report, and can save the configuration as a customized report instance for future re-use.

Details and criteria are set in multiple sections. Every type of report includes a **Standard Properties** and **Report Layout** section, as the first and last sections, respectively.

Parameters that are specific to a given report are defined in one or more sections between these two. Navigate between the “section” pages by clicking the section in the Sections list, or by clicking **Next** and **Previous** at the bottom of the Edit Report page.

See:

Standard Report Properties

Report-Specific Parameters

Saving and Executing Report Instances

Report Layout

See Also:

Scheduled Reports Tab

Report Results Tab

Standard Report Properties

All reports use a set of standard properties for basic information, such as name and description, and for setting controls such as email recipients and required signoff.

> The Name field is required for all reports; the other standard properties are optional.

Enter or edit the standard properties information as required when creating or editing a report.

Field	Description
Name	Name of the report.
Description	Brief description of the report.
Require Signoff	Require signoff on the results of this task. Reports that require sign off generate work items and email notifications that are assigned to the designated signers. Signoff decisions are stored with the report results for tracking purposes.
Previous Result Action	Previous result actions determine how subsequent runs of this report affect existing report results. **Delete** — overwrite the previous report results with the new information. **Rename Old** — append a numeral to the name of the old report result. **Rename New** — append a numeral to the name of the new report result. **Cancel** — cancel the new run of the report if a report result with the same name exists.
Allow Concurrency	Enable two identical reports to run at the same time. If enabled, allow concurrency appends a numeric value to the name of the report that started second. If disabled, the second report is canceled and an exception is sent to the requester.
Email Recipient	Specify a user or workgroup to whom an email should be sent when the report is finished running. Sending an email notification removes the need to log in to the product to check the progress of long-running reports or reports that are scheduled to run periodically.
Email Attachment Format	Select either or both check boxes for PDF or CSV to have the report include an attachment copy. Clear the check boxes to not receive an attachment.
Don't email empty reports	If the report is empty, do not email the report.
Maximum results to display	Set the maximum number of results to display in the results report. This option is available on a limited number of reports.
Scope	Set the scope for this report. Scope control access. Only identities that control the scope specified can see the results of this report. The scope information is not available for all reports. For those reports that support this feature, the Administrator must enable and configure the scope option.

For a list of available report templates, see Report List

Report Layout

The Report Layout section of the Summary panel on the Edit Reports page is where you design the visible structure of your reports.

Field	Description
Sort by	Use the drop-down list to select the criteria by which the report is sorted.
Group by	Use the drop-down list to select the criteria by which the report is grouped. The resulting report displays the data in collapsible groups.
Columns	The column names to the right are all the possible columns the report can contain. Click to select a column name and either drag and drop, or use the up/down arrow keys to arrange the order in which you want the columns to appear in the report. To prevent a column from appearing in the report, click to select the column name then click the left arrow button to move it to the panel on the left. All the columns listed in the right panel appear in the final report.
Disable Report Parameters Display	Report parameters are included in the report results by default. Select this option to disable the display of report parameters in the report results.
Disable Report Summary Display	Select this option to disable the display of a summary in the report results.
Disable Report Detail Display	Select this option to disable the display of a report details in the report results.
Include Report Parameters in CSV File	Select this option to include report parameter names and values in the CSV file, as comments. These comments are preceded with a # character. This output may not be compatible with some CSV parsers.

For a list of available report templates, see Report List

Report-Specific Parameters

Most reports offer at least one page of configuration options between the Standard Properties and Report Layout pages. These pages can be different for each report, and some reports use several pages, while others include only one. These pages allow the user to set filter parameters for the report instance. For example, the Uncorrelated Accounts Report contains one report-specific settings page called **Uncorrelated Accounts Parameters**; this page lets the user select the **Application** for which they want to see a list of accounts that could not be correlated to existing Identities (from the authoritative application). If no application is selected in this filter, the report shows all uncorrelated accounts from all applications.

In some cases, the **Report Layout** column list will change based on the parameters that are set on the report-specific parameters pages. For example, the **User Account Attributes Report** can display account attributes on selected applications. If the application selected has attributes (for example, privileged or service accounts) which other applications don't have, when that application is selected for the report, those columns appear on the Report Layout page for optional inclusion in the report.

Saving and Executing Report Instances

Once a report has been customized with filtering parameters, sorting and grouping choices, and layout preferences, it can be saved as a My Reports report instance for future use/re-use. There are several save options available:

- **Save**: saves the report instance, with its parameters and options, to the My Reports tab, using the name provided on the Standard Properties window
- **Save and Preview**: saves the report instance to the My Reports tab and runs a preview of the report, which displays the summary section (unless suppressed) and the first page of detail results (20 records); this allows the user to verify that the report shows the data they want to see; this option does not save the report results for later viewing
- **Save and Execute**: saves the report specification to the My Reports tab and runs the report; the report results are saved to the database and can be recalled from the Report Results tab until they are deleted

Modifying in the Preview Mode

The **Save and Preview** option lets you modify the report output layout, including rearranging columns, changing the detail sort order, and hiding either the summary or detail section. Any changes made in preview mode can be saved to the report specification, allowing Preview mode to function as an interactive method of reconfiguring the report output. A message at the top of the report prompts the user to choose whether to **Save Changes** or **Cancel Changes** when they alter the appearance of the report preview.

When a report is executed (as opposed to previewed), the final results cannot be reordered in the on-screen display of the report. The report can, however, be downloaded as a CSV and manipulated in a spreadsheet application as needed.

Reports Without a Preview Option

A few of the reports cannot be viewed in preview mode; this is because the data in these reports cannot be polled without fully executing the report. For example, the **Identity Forwarding Report** shows the forwarding user for all Identities who have one specified. Because the forwarding property is not searchable, these cannot be counted up front, and the report cannot be previewed. In some cases, a report can be previewed unless certain options on it are selected. The **Manager Access Review Report**, for example, can be previewed unless the **Show Excluded Items** option is selected. In these cases, a message is shown indicating that preview is not available when the user clicks **Save and Preview**.

My Reports Tab

The My Reports tab lists any customized reports that you have created and saved based on a report template. When customized report instances are saved, they appear in the list for the user. The first time a user access the Reports page, the My Reports will be empty; once you have created and saved customized reports they will be listed here.

You can use the **Search by Report Name** field to find the report you want to run. The **Filter searches by** setting in the **gear menu > Global Settings > IdentityIQ Configuration > Miscellaneous** tab, in the **Reporting** section, determines whether the search will find only reports that *start with* the string you entered, or reports that *contain* the string anywhere in the name.

From this page, any report instance can be opened, edited to change details and filtering criteria, and saved with updates (with or without running the report). Instances can also be used to create new report instances and can be run, scheduled, or deleted through their right-click menu options. The right-click menu options are:

- **Save as New Report** — Creates a new report instance based on an existing instance. Changes made are saved as a new report instance, leaving the existing one intact. This is helpful when a report offers a large number of configuration parameters and a new instance is being created that changes only a few of the options

(filters, sorts, etc.).
- **Edit** — Edits the existing report instance. This is the same as clicking the report instance in the list
- **Schedule** — Schedules the report instance for future (or repeated) execution.
- **Execute** — Runs the report instance immediately.
- **Delete** — Deletes the instance's configuration from IdentityIQ.

Scheduled Reports Tab

When you choose the option to schedule a report template or instance to run later (right-click > **Schedule**), the **New Schedule** page is displayed. You must enter a name for the scheduled version of the report, and can optionally add a description. You can choose a date and time to run the report, and can set the report to run at various frequencies (once, hourly, daily, weekly, monthly, quarterly, or annually).

Use the **Search by Schedule Name** field to find the scheduled report you want to run. The **Filter searches by** setting in the **gear menu > Global Settings > IdentityIQ Configuration > Miscellaneous** tab, in the **Reporting** section, determines whether the search will find only reports that *start with* the string you entered, or reports that *contain* the string anywhere in the name.

Reports that have been scheduled for future or repeated execution are listed on the **Scheduled Reports** tab. Once the scheduled report has run for the last time (for example, it was originally scheduled to run one time, at a specific date and time, and that time arrived, so it ran), it is removed from this list; only future-scheduled report executions are shown on this page.

Report Results Tab

The **Report Results** tab shows the completion status of all reports that have run and are currently available for viewing.

Use the **Search by Result Name** field to find the report results you want to view. The **Filter searches by** setting in the **gear menu > Global Settings > IdentityIQ Configuration > Miscellaneous** tab, in the **Reporting** section, determines whether the search will find only reports that *start with* the string you entered, or reports that *contain* the string anywhere in the name.

Click any report in the list to view its results. From the Report Result window, the report can be viewed on screen, downloaded as a PDF, or downloaded as a CSV file.The PDF and CSV forms of the report are created during report execution and saved to the database, making the download of either format fast and efficient.

XML Representation of Reports and Instances

Standard report templates are represented in the IdentityIQ object model as TaskDefinition objects. The XML representation of these can be seen in the IdentityIQ Debug pages by selecting Task Definition from the **Object Browser** list and searching for the report's name in the **Name** column.

When a report is saved as a customized instance, a new XML object is created in the system to represent its custom configuration. The instance's XML is far simpler than the template's because it references the template for most of the report generation details.

Details on these XML representations are explored further in Developing Custom Reports.

Report Use

Your level of access determines what information is displayed on each page and tab.

Use IdentityIQ reporting to collect the information you need to manage the compliance process. Reporting replaces manual searches for data located in various systems around your enterprise.

SailPoint provides a number of standard reports that can be run without changes. You can also use the standard reports to create custom reports that are specific to your needs.The provided reports are displayed on the Reports tab. The following types of report templates are provided:

- **Detailed Reports** — include key data about specific areas in IdentityIQ. The information can be presented in table or grid format. The results can be exported to a .csv file and used in spreadsheets.
- **Archived Reports** — include end-of-period and task information that is formatted for easy dissemination of key audit information. Due to the large amount of data that is generated, the best option is to export the report results to a .pdf file
- **Summary Report** —include end-of-period and task information that is formatted for easy dissemination of key audit information. Due to the large amount of data that is generated, the best option is to export the report results to a .pdf file

The Reports page has the following tabs:

- My Reports Tab — displays all of the reports that you created.
- Reports Tab — view all reports created for your enterprise, or create new reports.
- Scheduled Reports Tab — view all reports scheduled to run.
- Report Results Tab — view the results of previous reports.

My Reports Tab

The My Reports tab displays all of the reports that you created using the templates, or standard reports, provided on the Reports tab. These reports are only available for your use. You can use scoping to make the results visible to other users.

Reports are listed by category. Use filtering to limit the number of reports displayed in the table. Enter a letter, or partial name in the **Search** field to display reports with names containing that letter pattern.

For a complete list of the report templates provided, see Report List.

Use this page to edit, run, schedule, export or delete your custom reports. Right-click the report name and select an option from the pop-up menu. When you select an export function, the report is run and the results are displayed in the selected format. For Detailed and Summary type reports the **Export to CSV** option is not available.

For more information, see Working With Reports.

To view a list of all scheduled reports, see Scheduled Reports Tab.

To view reports after they are completed, see Report Results Tab.

To create reports based on searches on identity, activity, and audit information, see the **Search** documentation.

The Reports page includes the following:

Column	Description
Name	The name of the report as defined when the report was created.
Description	A brief description of the specific report.

Reports Tab

SailPoint provides a number of standard reports that can be run without changes or that can be used as templates to create custom reports. The provided reports are displayed on the Reports tab. Three types of report templates are provided and include, Detail, Archive, and Summary reports.

> You cannot write over the report templates on the Reports tab. If you edit a report template from Reports tab and save the changes, you must assign a name to the new report and it is added to the report list on the My Reports tab.

Reports are listed by category. Use filtering to limit the number of reports displayed in the table. Enter a letter, or partial name in the **Search** field to display reports with names containing that letter pattern.

For a complete list of the report templates provided, see Report List.

Use this page to create, edit, run, schedule, export or delete your custom reports. Right-click the report name and select an option from the pop-up menu. When you select an export function, the report is run and the results are displayed in the selected format. For Detailed and Summary type reports the **Export to CSV** option is not available. For more information, see Working With Reports.

To view a list of all scheduled reports, see Scheduled Reports Tab.

To view reports after they are completed, see Report Results Tab.

To create reports based on searches on identity, activity, and audit information, see the **Search** documentation.

The Reports page includes the following:

Column	Description
Name	The name of the report template.
Description	A brief description of the specific report.

Report Results Tab

The Report Results page displays a list of reports run in the IdentityIQ application to which you have access. If scoping is active you may only have access to reports in scopes that you control.

Use the **Search by Result Name** field to find the report results you want to view. There is a **Filter searches by** setting in the **gear menu > Global Settings > IdentityIQ Configuration > Miscellaneous** tab, in the **Reporting** section, which determines whether the search will find only reports that *start with* the string you entered, or reports that *contain* the string anywhere in the name. See the IdentityIQ **System Configuration** documentation for details.

You can also use filtering options to limit the number of reports displayed in the table based on the date the report was run, and the report results (Success, Warning, Fail, or Cancelled)

The list of reports on this tab includes the following details for each report:

Column	Description
Name	The name of the report.
Date Complete	The date and time stamp of when the report completed running.
Result	The result status, Pending, Successful, or Failed.
Signoff	The status of the sign off request for the report results. **None** — no sign off required **Waiting** — sign off request not complete **Signed** — a sign off decision has been made
Owner	The user that created the report.

You can right-click on any report in this list and choose **View** to see details about that report, as well as the information collected. From this view, the report can be viewed on screen, downloaded as a PDF, or downloaded as a CSV file. The PDF and CSV forms of the report are created during report execution and saved to the database, making the download of either format fast and efficient.

> Export report names are cropped at 31 characters.

If a report was scheduled to run but there were no results, navigate to the Scheduled Reports Tab to check for any errors that might have occurred when the report was run.

To delete report results, right-click the result and select **Delete**. Reports that require a sign off can only be deleted by a user with the Signoff Administrator capability.

Working With Reports

The most common report tasks include the following:

- How to Create a New Report
- How to Run a Report
- How to Edit a Report
- How to Schedule a Report
- How to Complete Report Work Items

You can also select one of the export features to launch a report and export the results directly to an external file. Exported reports are not included in the list on the View Report Results page.

Report Work Items

Reports that require sign off generate work items and email notifications that are assigned to the designated signers. Sign off decisions are retained with the report results for tracking purposes.

New Reports

To create a new report, on the Reports tab, click an existing report or right-click and select **Save As New Report** display the New Report page.

Existing Reports

To edit an existing report on the My Reports tab, click a report name or right-click and select **Edit** to display the Edit Report page.

To edit reports based on searches on identity, activity, and audit information, see the **Search** documentation.

Scheduled Reports

To schedule a report to run at a later time or on a recurring basis, right-click a report name and select **Schedule** from the drop-down list to display the New Schedule dialog. You can schedule reports to run once, hourly, daily, weekly, monthly, quarterly or annually to meet the requirements of your enterprise and auditors.

To delete a report, right-click the report name and select **Delete** from the drop-down menu. Click **Yes** on the confirmation pop-up to delete the report. When you delete a report from the Reports table, all associated report results are deleted as well.

How to Create a New Report

Use the New Report page to create reports for your organization based on the reports provided. Reports can be as general (all users in your organization) or specific (one user) as required.

See Standard Report Properties for the complete list of reports provided with IdentityIQ.

Searches defined on the search pages can also be saved as reports. Reports created on the search pages are saved in the Search category on the My Reports tab.

Procedure

1. Access the Reports page from the navigation menu bar. Go to **Intelligence -> Reports**.
2. Right-click a report on the My Reports or Reports tab and select **Save As New Report**.
3. Enter a name and brief description of the new report.
   This information is displayed on the My Reports table when the new report is saved.
4. *Optional*: Require sign off.
   a. Activate Required sign off to expand the Signoff Properties section.
   b. Specify the required signers. Enter the first letter, or letters, of an identity to display a selection list of valid identities containing that letter string and select a signer.
   c. Click Add to List to add the identity to the signers list. You can add as many signers as are required.
   d. Select an email notification template from the Initial Notification Email drop-down list. For example, the Report Result Signoff template. Templates are created and defined when the application is configured.
   e. Specify the escalation criteria for the sign off request.
      - **None** — no reminder emails are sent and no escalation is performed for this work item.
      - **Send Reminders** — email reminders are sent at the configured interval.
      - **Reminders then Escalation** — the configured number of reminders are sent and then the work item is escalated to the signers manager.
      - **Escalation only** — this work item is escalated after the configured interval with no reminders being sent.
      - Escalation intervals are set when the application is configured.
5. Select a **Previous Result Action** from the drop-down list. **Rename Old** is select by default. Previous result actions determine how subsequent runs of this report react to existing report results.
   a. **Delete** — overwrite the previous report results with the new information.
   b. **Rename Old** — append a numeral to the name of the old report result and preserve both.
   c. **Rename New** — append a numeral to the name of the new report result and preserve both.
   d. **Cancel** — cancel the new run of the report.

6. *Optional*: Allow concurrency. Activate the **Allow Concurrency** check box to enable two identical reports to run at the same time.
    - If enabled, allow concurrency appends a numeric value to the name of the report that started second.
    - If disabled, the second report is canceled and an exception sent to the requestor.
7. *Optional*: Assign an email recipient to receive notification of report completion. Enter the first letter, or letters, of an identity to display a selection list of valid identities containing that letter string, or click the arrow to the right of the field to display a list of all users. To prevent an email being sent if the report is empty, check **Don't email empty reports**.
8. *Optional*: Enter the maximum number of results to display in the report results.
9. *Optional*: Enter a scope for the report results. Enter the first few letters of a scope name to display the select box, or click the arrow to the right of the field to display all of the scope you control. Only identities that control the assigned scope can view the results of a scoped report.
   If scope is active and you do not explicitly assign a scope, the results are given your assigned scope.
10. Specify the report options required for the report you are creating.
    Each report type displays unique report options. **See Report List for details on each report type.**
11. Specify how the information will display in the report results.
12. Choose an option to save and/or run the report:
    - Click **Save** to save the new report to the My Reports table.
    - Click **Save and Execute** to save the report to the My Reports table and run it immediately. The Report Results page displays when the report completes.
    - Click **Save and Preview** to preview the report results.
    - Click **Execute** to run without saving.

For more information on report results, see Report Results Tab

How to Run a Report

Right-click the report name and select **Execute** or **Execute in background**. **Execute** displays a pop-up progress window and opens the Report Results page when it is complete. **Execute in background** launches the report in the background. To track progress or to view the finished report, navigate to the Report Results tab.

Procedure

1. Access the Reports page from the navigation menu bar. Go to **Intelligence -> Reports**.
2. Navigate to the My Reports tab to view a list of your saved reports.
3. Right-click a report and select **Execute** or **Execute in background**.
   Execute displays a pop-up progress window and opens the Report Results page when it is complete. **Execute in background** launches the report in the background.
4. To track progress or to view the finished report, navigate to the Report Results tab.

For more information on report results, see Report Results Tab

How to Edit a Report

Use the Edit Report page to make changes to an existing report.

Procedure

1. Access the Reports page from the navigation menu bar. Go to **Intelligence -> Reports**.
2. Navigate to the My Reports tab to view a list of your saved reports.
3. Click a report, or right-click a report and select **Edit** from the drop-down list to open the Edit Report page.
4. Edit the **Name** and **Description** section as needed.
5. Select a **Previous Result Action** from the drop-down list. **Rename Old** is select by default. Previous result actions determine how subsequent runs of this report react to existing report results.

- **Delete** — overwrite the previous report results with the new information.
- **Rename Old** — append a numeral to the name of the old report result and preserve both.
- **Rename New** — append a numeral to the name of the new report result and preserve both.
- **Cancel** — cancel the new run of the report if a report result with the same name exists.

6. *Optional*: Allow concurrency. Activate the **Allow Concurrency** check box to enable two identical reports to run at the same time.
   - If enabled, allow concurrency appends a numeric value to the name of the report that started second.
   - If disabled, the second report is canceled and an exception sent to the requestor.
7. *Optional*: Assign an email recipient to receive notification of report completion. Enter the first letter, or letters, of an identity to display a selection list of valid identities containing that letter string, or click the arrow to the right of the field to display a list of all users. To prevent an email being sent if the report is empty, check **Don't email empty reports**.
8. *Optional*: Require sign off.
   a. Activate Required sign off to expand the Signoff Properties section.
   b. Specify the required signers.
      Enter the first letter, or letters, of an identity to display a selection list of valid identities containing that letter string and select a signer.
   c. Click Add to List to add the identity to the signers list.
      You can add as many signers as are required.
   d. Select an email notification template from the Initial Notification Email drop-down list. For example, the Report Result Signoff template.
      Templates are created and defined when the application is configured.
   e. Specify the escalation criteria for the sign off request.
      None — no reminder emails are sent and no escalation is performed for this work item.
      Send Reminders — email reminders are sent at the configured interval.
      Reminders then Escalation — the configured number of reminders are sent and then the work item is escalated to the signers manager.
      Escalation only — this work item is escalated after the configured interval with no reminders being sent.
      Escalation intervals are set when the application is configured.
9. *Optional*: Enter the maximum number of results to display in the report results. This option is available on a limited number of reports.
10. *Optional*: Enter a scope for the report results. Enter the first few letters of a scope name to display the select box, or click the arrow to the right of the field to display all of the scope you control.
    Only identities that control the assigned scope can view the results of a scoped report.
    If scope is active and you do not explicitly assign a scope, the results are given your assigned scope. See Report List for details on each report type.
11. Choose an option to save and/or run the report:
    - Click **Save** to save the new report to the My Reports table.
    - Click **Save and Execute** to save the report to the My Reports table and run it immediately. The Report Results page displays when the report completes.
    - Click **Save and Preview** to preview the report results.
    - Click**Execute** to run without saving.
12. Click **Save** to save the new report to the My Reports table.
    - Click **Save and Execute** to save the report to the My Reports table and run it immediately.
      The Report Results page displays when the report completes.
    - Click **Save and Preview** to preview the report results.
    - Click **Execute** to run without saving.

See also:

Standard Report Properties

Report Layout

Report Results Tab

How to Schedule a Report

Use the Schedule Report dialog to schedule reports to run at slow processing times or on a recurring basis as need to maintain compliance in your enterprise.

The New Schedule dialog enables you to assign a unique name and description to the report being run at the schedule time. The unique schedule name and description display on the Report Results table so that a report run from the Reports page does not overwrite the scheduled report. For example, if you define and schedule a Weekly All Violations Report that you download and archive for auditing purposes, someone running the All Violations Report mid-week does not overwrite the information in your scheduled report.

Procedure

1. Access the Reports page from the navigation menu bar. Go to **Intelligence > Reports**.
2. Right-click a report name on the My Reports or Reports tabs and select **Schedule** from the drop-down list to open the New Schedule dialog.
3. Enter a unique name and description for this schedule report.
   This is the name and description that display in the Report Results table and distinguish this scheduled version of the report from the same report executed from the reports tables. Defining a unique name on this page ensures that scheduled reports are not overwritten by mistake.
4. Enter the date and time to launch the first execution of this report. You can enter the date manually, or click the **...** icon to select a date from the calendar.
   — OR —
   Select the **Run Now** field to run the report immediately after clicking **Schedule**. For recurring reports, the report runs at the current time at the specified **Execution Frequency**.
5. Specify how often this report should run with the **Execution Frequency** drop-down list. Subsequent executions of this report occur at the time specified in the **First Execution** fields.
6. Click **Schedule** to save this scheduled report.
7. Navigate to the Scheduled Reports Tab to view a list of all scheduled reports in the IdentityIQ application.

How to Complete Report Work Items

Report work items are generated by reports that require sign off on the results they create and those sign off requests that are forwarded by a designated signer.

Sign off decisions are retained with the report results for tracking purposes.

Procedure

1. Click **My Work** in the Navigation menu to view your current work items.
2. Click a sign off type work item to display the sign off request.
3. Review the work item information in the Summary section.
4. Review the Comments section for any information associated with this work item.
5. Use the **Add Comment** button to add additional information to the work item if necessary.
6. In the Details sections, click **Click to View Report Results** to display the Report Results page.
7. After you complete your review of the report results, click **Return to Work Item**.
8. Click an action button to open the associated comments dialog and conclude this work session.

If you sign off or reject the sign-off request, the status of the report results is updated to reflect that decision. If you forward the work item, you must specify a recipient.

Report List

SailPoint provides a number of standard reports that can be run without changes. You can also use the standard reports to create custom reports that are specific to your needs. Use scope to control access to your report results.

All reports use a set of standard properties for basic information, such as naming and descriptions, and to set controls, such as scope and to required sign off. The Report Layout configuration procedure is the same for all reports. See the following:

The reports are divided in to the following categories:

- Access Review and Certification Reports
- Activity Reports: User Activity Detailed Report
- Administration Reports
- Application Status Report
- Configured Resource Reports
- Identity and User Reports
- Lifecycle Manager Reports - for details, see the **Lifecycle Manager** documentation
- Policy Violation Report
- Risk Reports
- Role Management Reports

For step by step instructions on creating or editing a report, see Working With Reports

Access Review and Certification Reports

- Access Review Decision Report
- Access Review Signoff Live Report
- Account Group Access Review Live Report
- Advanced Access Review Live Report
- Application Owner Access Review Live Report
- Certification Activity by Application Report
- Entitlement Owner Access Review Live Report
- Manager Access Review Live Report
- Role Composition Access Review Live Report
- Targeted Access Review Live Report

Access Review Decision Report

The Access Review Decision Report includes information about the decisions made by certifiers for all items in non-archived access reviews that match the report criteria.

Report results are presented in several pages. The first page shows a summary, divided into two sections:

- the **Certification Statistics** section shows a count of certifications of each type and the number of certification entities (e.g. identities, roles, account groups) and unique entities included in each certification category;
- the **Decision Statistics** section shows the number of approved items, revoked items, allowed exceptions, and total decisions for each type of certification item type.

The pages following the summary show details of each access review in the report, displaying each certification entity and all certification items with the decisions that are currently recorded for each. The **Decision Maker** shows the user who actually made the certification decision, which may be someone other than the original certifier if the review was

delegated, reassigned, or forwarded. The **Decision** column also indicates if the decision was made as part of a bulk certification, if that option was permitted by the installation's configuration.

This report is an archive-type report. Archive reports include end-of-period and task information that is formatted for easy dissemination of key audit information. Due to the large amount of data that is generated, the best option is to export the report results to a .pdf file.

All reports use a set of standard properties for basic information, such as naming and descriptions, and to set controls, such as scope and to required sign off.

You must enter the following before running this report:

- Name

For more information on Standard Properties, see Standard Report Properties

For more information on Report Layout, see Report Layout

For step by step instructions on creating or editing a report, see Working With Reports

Report Criteria

The following criteria determines what information is included in this report.You can use any combination of options to build a report.

> Selecting NO options from a list indicates that ALL options in the list are included in the report.

Option	Description
Creation Start and End Date (s)	The access review creation date range. The report includes all access reviews create on or after the start date and on or before the end date. You can enter the date manually, or click the **"..."** icon to select a date from the calendar.
Signed Start and End Date (s)	The access review signed off on date range. The report includes all access reviews signed off on, on or after the start date and on or before the end date. You can enter the date manually, or click the **"..."** icon to select a date from the calendar.
Due Start and End Date(s)	The access review due date range. The report includes all access reviews due on or after the start date and on or before the end date. You can enter the date manually, or click the **"..."** icon to select a date from the calendar.
Tags	To filter access reviews based on their tags, select one or more tags. If multiple tags are selected, only access reviews that match *all* selected tags are included in this report.
Applications	Select the applications to include in the report. If no applications are specified, all applications are included. Click the arrow to the right of the suggestion field to display a list of all applic-ations, or enter a few letters in the field to display a list of applications that start

Option	Description
	with that letter string.
Managers	The manager list to include in this report. If no managers are specified, access reviews for all managers are included. Click the arrow to the right of the suggestion field to display a list of all managers, or enter a few letters in the field to display a list of managers that start with that letter string.

Access Review Signoff Live Report

The Access Review Signoff Live Report includes information on who signed off on a access review and if the signoff was completed. It shows the names of the signers (if any) and the signoff dates and indicates whether the reviews were electronically signed, along with the corresponding signature meaning. It also shows basic information about each access review, such as its name, the name of its parent certification, start date, due date, the access review owner, and tags associated with the review.

This report includes information in the detailed results format that can be exported to a .csv file and used as spreadsheets.

The Access Review Signoff Live Report consists of the following sections:

- Standard Report Properties
- Report Options. These options are described in the Certification Properties table below.
- Report Layout

All reports use a set of standard properties for basic information, such as naming and descriptions, and to set controls, such as scope and to required sign off.

You must enter the following before running this report:

- Name

For step by step instructions on creating or editing a report, see Working With Reports

Certification Properties

The following criteria determines what information is included in this report. You can use any combination of options to build a report.

> Selecting NO options from a list indicates that ALL options in the list are included in the report.

Option	Description
Creation Start and End Date (s)	The access review creation date range. The report includes all access reviews create on or after the start date and on or before the end date. You can enter the date manually, or click the **"..."** icon to select a date from the calendar.
Signed Start	The access review signed off on date range. The report includes all access

Option	Description
and End Date (s)	reviews signed off on, on or after the start date and on or before the end date. You can enter the date manually, or click the **"..."** icon to select a date from the calendar.
Due Start and End Date(s)	The access review due date range. The report includes all access reviews due on or after the start date and on or before the end date. You can enter the date manually, or click the **"..."** icon to select a date from the calendar.
Managers	The manager list to include in this report. If no managers are specified, access reviews for all managers are included. Click the arrow to the right of the suggestion field to display a list of all managers, or enter a few letters in the field to display a list of managers that start with that letter string.
Applications	Select the applications to include in the report. If no applications are specified, all applications are included. Click the arrow to the right of the suggestion field to display a list of all applications, or enter a few letters in the field to display a list of applications that start with that letter string. Only access reviews for account groups on the selected applications are included in the report.
Groups	The groups to include in the report. Click the "x" next to an item in the inclusion list to remove it from the report.
Certification Tags	To filter access reviews based on their tags, select one or more tags. If multiple tags are selected, only access reviews that match all selected tags are included in this report.
Certification Group	The manager certifications to include in this report.
Signed Off	Filter by the signed off status of certifications.
E-Signed	Use this field to filter results by certifications that include an electronic signature.

Account Group Membership Access Review Live Report

This report shows line item details of all account group membership access reviews which meet the filter criteria. The purpose of this report is to show the decisions made on each item along with the decision maker's name and comments and the current status of any applicable revocations. It also includes basic identifying information for the account group and member (such as account number, identity, application, and account group name).

This report includes information in the detailed results format that can be exported to a .csv file and used as spreadsheets.

The Account Group Access Review Live Report consists of the following sections:

- Standard Report Properties
- Certification Properties. These options are described in the table below.
- Report Layout

All reports use a set of standard properties for basic information, such as naming and descriptions, and to set controls, such as scope and to required sign off.

You must enter the following before running this report:

- Name

For step by step instructions on creating or editing a report, see Working With Reports

Certification Properties

The following criteria determines what information is included in this report.You can use any combination of options to build a report.

> Selecting NO options from a list indicates that ALL options in the list are included in the report.

Option	Description
Creation Start and End Date (s)	The access review creation date range. The report includes all access reviews create on or after the start date and on or before the end date. You can enter the date manually, or click the **"..."** icon to select a date from the calendar.
Signed Start and End Date (s)	The access review signed off on date range. The report includes all access reviews signed off on, on or after the start date and on or before the end date. You can enter the date manually, or click the **"..."** icon to select a date from the calendar.
Due Start and End Date(s)	The access review due date range. The report includes all access reviews due on or after the start date and on or before the end date. You can enter the date manually, or click the **"..."** icon to select a date from the calendar.
Applications	The applications to include in the report. If no applications are specified, all applications are included. Click the arrow to the right of the suggestion field to display a list of all applications, or enter a few letters in the field to display a list of applications that start with that letter string. Only access reviews for account groups on the selected applications are included in the report.
Certification Tags	To filter access reviews based on their tags, select one or more tags. If multiple tags are selected, only access reviews that match all selected tags are included in this report.
Certification Groups	The type of Account Group access reviews to include in this report, Membership or Permissions.
Show excluded items	Show items that were excluded from the certification through a rule or other criteria.

Option	Description
	Note: This option disables the preview grid view and the option to sort by Status, Decision, Decision Maker, Application, or Recommendation.

Account Group Permissions Access Review Live Report

This report shows line item details of all account group permissions access reviews which meet the filter criteria. The purpose of this report is to show the decisions made on each item along with the decision maker's name, any comments, and the current status of any applicable revocations. It also includes basic identifying information about each account group and permission (account group name, application, and permission).

This report includes information in the detailed results format that can be exported to a .csv file and used as spreadsheets.

The Account Group Access Review Live Report consists of the following sections:

- Standard Report Properties
- Certification Properties. These options are described in the Certification Properties table below.
- Report Layout

All reports use a set of standard properties for basic information, such as naming and descriptions, and to set controls, such as scope and to required sign off.

You must enter the following before running this report:

- Name

For step by step instructions on creating or editing a report, see Working With Reports

Certification Properties

The following criteria determines what information is included in this report.You can use any combination of options to build a report.

> Selecting NO options from a list indicates that ALL options in the list are included in the report.

Option	Description
Creation Start and End Date (s)	The access review creation date range. The report includes all access reviews create on or after the start date and on or before the end date. You can enter the date manually, or click the **"..."** icon to select a date from the calendar.
Signed Start and End Date (s)	The access review signed off on date range. The report includes all access reviews signed off on, on or after the start date and on or before the end date. You can enter the date manually, or click the **"..."** icon to select a date from the calendar.
Due Start and End Date(s)	The access review due date range. The report includes all access reviews due on or after the start date and on or before the end date.

Option	Description
	You can enter the date manually, or click the **"..."** icon to select a date from the calendar.
Applications	The applications to include in the report. If no applications are specified, all applications are included. Click the arrow to the right of the suggestion field to display a list of all applications, or enter a few letters in the field to display a list of applications that start with that letter string. Only access reviews for account groups on the selected applications are included in the report.
Certification Tags	To filter access reviews based on their tags, select one or more tags. If multiple tags are selected, only access reviews that match all selected tags are included in this report.
Certification Groups	The type of Account Group access reviews to include in this report, Membership or Permissions.
Show excluded items	Show items that were excluded from the certification through a rule or other criteria. **Note: This option disables the preview grid view and the option to sort by Status, Decision, Decision Maker, Application, or Recommendation.**

Advanced Access Review Live Report

The Advanced Access Review Live Report includes information on all non-archived advanced access reviews that match the criteria specified. The purpose of this report is to show the decisions made on each item, along with the decision maker's name and comments and the current status of any applicable revocations. It also includes basic identifying information about each line item (account name, identity first and last name, manager's name, entitlement type and value, application, and instance).

This report includes information in the detailed results format that can be exported to a .csv file and used as spreadsheets.

The Advanced Access Review Live Report consists of the following sections:

- Standard Report Properties
- Certification Properties. These options are described in the table below.
- Report Layout

All reports use a set of standard properties for basic information, such as naming and descriptions, and to set controls, such as scope and to required sign off.

You must enter the following before running this report:

- Name

For step by step instructions on creating or editing a report, see Working With Reports

Certification Properties

The following criteria determines what information is included in this report. You can use any combination of options to build a report.

> Selecting NO options from a list indicates that ALL options in the list are included in the report.

Option	Description
Creation Start and End Date(s)	The access review creation date range. The report includes all access reviews create on or after the start date and on or before the end date. You can enter the date manually, or click the **"..."** icon to select a date from the calendar.
Signed Start and End Date (s)	The access review signed off on date range. The report includes all access reviews signed off on, on or after the start date and on or before the end date. You can enter the date manually, or click the **"..."** icon to select a date from the calendar.
Due Start and End Date(s)	The access review due date range. The report includes all access reviews due on or after the start date and on or before the end date. You can enter the date manually, or click the **"..."** icon to select a date from the calendar.
Groups	The groups or populations to include in the report. Click the arrow to the right of the field and select **Populations**, to display a select list of populations, or select a group factory name to display a select list of groups created by that factory. Click on populations and groups from the select lists to create the inclusion list for this report. Click an item in the inclusion list to remove it from the report.
Certification Tags	To filter access reviews based on their tags, select one or more tags. If multiple tags are selected, only access reviews that match all selected tags are included in this report.
Certification Group	The manager certifications to include in this report.
Show excluded items	Show items that were excluded from the certification through a rule or other criteria. **Note: This option disables the preview grid view and the option to sort by Status, Decision, Decision Maker, Application, or Recommendation.**

Application Owner Access Review Live Report

The Application Owner Access Review Live Report includes information on all non-archived application owner access reviews that match the criteria specified. The purpose of this report is to show the decisions made on each item, along with the decision maker's name and comments and the current status of any applicable revocations.

The report includes a summary section at the top which provides summary counts of certifications, access reviews, identities, and certification items included in the report and then illustrates counts of item decisions reported by entitlement type (role, additional entitlement), representing each decision type(open, approved, and revoked) in a separate column in the graph.

The report body shows the decisions made on each item along with the decision maker's name and comments and the current status of any applicable revocations.

This report includes information in the detailed results format that can be exported to a .csv file and used as spreadsheets.

The Application Owner Access Review Report consists of the following sections:

- Standard Report Properties
- Certification Properties. These options are described in the table below.
- Report Layout

All reports use a set of standard properties for basic information, such as naming and descriptions, and to set controls, such as scope and to required sign off.

You must enter the following before running this report:

- Name

For step by step instructions on creating or editing a report, see Working With Reports

Certification Properties

The following criteria determines what information is included in this report. You can use any combination of options to build a report.

> Selecting NO options from a list indicates that ALL options in the list are included in the report.

Option	Description
Creation Start and End Date (s)	The access review creation date range. The report includes all access reviews create on or after the start date and on or before the end date. You can enter the date manually, or click the **"..."** icon to select a date from the calendar.
Signed Start and End Date (s)	The access review signed off on date range. The report includes all access reviews signed off on, on or after the start date and on or before the end date. You can enter the date manually, or click the **"..."** icon to select a date from the calendar.
Due Start and End Date(s)	The access review due date range. The report includes all access reviews due on or after the start date and on or before the end date. You can enter the date manually, or click the **"..."** icon to select a date from the calendar.
Applications	Select the applications to include in the report. If no applications are specified, all applications are included.

Option	Description
	Click the arrow to the right of the suggestion field to display a list of all applications, or enter a few letters in the field to display a list of applications that start with that letter string. Only access reviews for the selected applications are included in the report.
Certification Tags	To filter access reviews based on their tags, select one or more tags. If multiple tags are selected, only access reviews that match all selected tags are included in this report.
Certification Group	The manager certifications to include in this report.
Show excluded items	Show items that were excluded from the certification through a rule or other criteria. **Note: This option disables the preview grid view and the option to sort by Status, Decision, Decision Maker, Application, or Recommendation.**

Certification Activity by Application Report

The Certification Activity by Application Report includes information activity performed on non-archived certifications that match the specified criteria. It excludes access reviews from role composition or account group permission certifications, since they are not identity-focused certifications. Depending on the filter criteria, the report may include some line items from a certification but omit other line items; for example, if an application is specified, only line items from a manager certification that relate to the specified application are included on the report.

The report body shows the decisions made on each item along with the decision maker's name and comments and the current status of any applicable revocations.

This report includes information in the detailed results format that can be exported to a .csv file and used as spreadsheets.

The Certification Activity by Application Report consists of the following sections:

- Standard Report Properties
- Certification Properties. These options are described in the table below.
- Report Layout

All reports use a set of standard properties for basic information, such as naming and descriptions, and to set controls, such as scope and to required sign off.

You must enter the following before running this report:

- Name
- Application from the list

For step by step instructions on creating or editing a report, see Working With Reports

Certification Properties

The following criteria determines what information is included in this report. You can use any combination of options to build a report.

Selecting NO options from a list indicates that ALL options in the list are included in the report.

Option	Description
Creation Start and End Date (s)	The access review creation date range. The report includes all access reviews create on or after the start date and on or before the end date. You can enter the date manually, or click the **"..."** icon to select a date from the calendar.
Signed Start and End Date (s)	The access review signed off on date range. The report includes all access reviews signed off on, on or after the start date and on or before the end date. You can enter the date manually, or click the **"..."** icon to select a date from the calendar.
Due Start and End Date(s)	The access review due date range. The report includes all access reviews due on or after the start date and on or before the end date. You can enter the date manually, or click the **"..."** icon to select a date from the calendar.
Applications	Select one application to include in this report, or leave this field blank to include all applications. To select an application, click the arrow to the right of the suggestion field to display a list of all applications, or enter a few letters in the field to display a list of applications that start with that letter string. **Note**: Selecting more than one application is not supported, and causes the report to render no results.
Certification Tags	To filter access reviews based on their tags, select one or more tags. If multiple tags are selected, only access reviews that match all selected tags are included in this report.
Certification Group	The manager certifications to include in this report.
Show excluded items	Show items that were excluded from the certification through a rule or other criteria. **Note: This option disables the preview grid view and the option to sort by Status, Decision, Decision Maker, Application, or Recommendation.**

Entitlement Owner Access Review Live Report

The Entitlement Owner Access Review Live Report includes information on all non-archived entitlement owner access reviews that match the criteria specified. The purpose of this report is to show the decisions made on each item along with the decision maker's name and comments and the current status of any applicable revocations.

The report includes a summary report at the top which shows a summary table of the number of certifications access reviews, identities, and certification items included in the report, along with a graph showing the relative counts of item decisions (e.g. open, approved, revoked).

The report body shows the each line item with its decision details and revocation status.

This report includes information in the detailed results format that can be exported to a .csv file and used as spreadsheets.

The Entitlement Owner Access Review Report consists of the following sections:

- Standard Report Properties
- Certification Properties. These options are described in the table below.
- Report Layout

All reports use a set of standard properties for basic information, such as naming and descriptions, and to set controls, such as scope and to required sign off.

You must enter the following before running this report:

- Name

For step by step instructions on creating or editing a report, see Working With Reports

Certification Properties

The following criteria determines what information is included in this report. You can use any combination of options to build a report.

> Selecting NO options from a list indicates that ALL options in the list are included in the report.

Option	Description
Creation Start and End Date (s)	The access review creation date range. The report includes all access reviews create on or after the start date and on or before the end date. You can enter the date manually, or click the **"..."** icon to select a date from the calendar.
Signed Start and End Date (s)	The access review signed off on date range. The report includes all access reviews signed off on, on or after the start date and on or before the end date. You can enter the date manually, or click the **"..."** icon to select a date from the calendar.
Due Start and End Date(s)	The access review due date range. The report includes all access reviews due on or after the start date and on or before the end date. You can enter the date manually, or click the **"..."** icon to select a date from the calendar.
Applications	Select the applications to include in the report. If no applications are specified, all applications are included. Click the arrow to the right of the suggestion field to display a list of all applications, or enter a few letters in the field to display a list of applications that start with that letter string. Only access reviews for the selected applications are included in the report.
Certification Tags	To filter access reviews based on their tags, select one or more tags. If multiple tags are selected, only access reviews that match all selected tags are included in this report.

Option	Description
Certification Group	The manager certifications to include in this report.
Show excluded items	Show items that were excluded from the certification through a rule or other criteria. **Note: This option disables the preview grid view and the option to sort by Status, Decision, Decision Maker, Application, or Recommendation.**

Manager Access Review Live Report

The Manager Access Review Report includes information on all non-archived manager access reviews that match the criteria specified. The purpose of this report is to show the decisions made on each item along with the decision maker's name and comments and the current status of any applicable revocations.

The report includes a summary report at the top which shows a summary table of the number of certifications, access reviews, identities, and certification items included in the report, along with a chart illustrating the counts of item decisions by type (e.g. open, approved, revoked, exception allowed), separated into the categories of roles, additional entitlements, and policy violations.

The report body shows the decisions made on each item along with the decision maker's name and comments and the current status of any applicable revocations.

This report includes information in the detailed results format that can be exported to a .csv file and used as spreadsheets.

All reports use a set of standard properties for basic information, such as naming and descriptions, and to set controls, such as scope and to required sign off.

The Manager Access Review Report consists of the following sections:

- Standard Report Properties
- Certification Properties. These are described in the table below.
- Report Layout

You must enter the following before running this report:

- Name

For step by step instructions on creating or editing a report, see Working With Reports

Certification Properties

The following criteria determines what information is included in this report. You can use any combination of options to build a report.

> Selecting NO options from a list indicates that ALL options in the list are included in the report.

Option	Description
Creation Start and End Date(s)	The access review creation date range. The report includes all access reviews create on or after the start date and on or before the end date. You can enter the date manually, or click the **"..."** icon to select a date from the calendar.
Signed Start and End Date (s)	The access review signed off on date range. The report includes all access reviews signed off on, on or after the start date and on or before the end date. You can enter the date manually, or click the **"..."** icon to select a date from the calendar.
Due Start and End Date(s)	The access review due date range. The report includes all access reviews due on or after the start date and on or before the end date. You can enter the date manually, or click the **"..."** icon to select a date from the calendar.
Managers	The manager list to include in this report. If no managers are specified, access reviews for all managers are included. Click the arrow to the right of the suggestion field to display a list of all managers, or enter a few letters in the field to display a list of managers that start with that letter string.
Certification Tags	To filter access reviews based on their tags, select one or more tags. If multiple tags are selected, only access reviews that match all selected tags are included in this report.
Certification Group	The manager certifications to include in this report.
Show excluded items	Show items that were excluded from the certification through a rule or other criteria. **Note: This option disables the preview grid view and the option to sort by Status, Decision, Decision Maker, Application, or Recommendation.**

Role Composition Access Review Live Report

This report includes information about all Role Composition Access Reviews in IdentityIQ. The Role Composition Access Review certifies that roles for which the reviewer is responsible are composed of the proper permissions and entitlements.

The purpose of this report is to show the decisions made on each item along with the decision maker's name and comments and the current status of any applicable revocations.

This report includes information in the detailed results format that can be exported to a .csv file and used as spreadsheets.

The Role Composition Access Review Report consists of the following sections:

- Standard Report Properties
- Certification Properties. These are described in the table below.
- Report Layout

All reports use a set of standard properties for basic information, such as naming and descriptions, and to set controls, such as scope and to required sign off.

You must enter the following before running this report:

- Name
- Role

For step by step instructions on creating or editing a report, see Working With Reports

Certification Properties

The following criteria determines what information is included in this report. You can use any combination of options to build a report.

> Selecting NO options from a list indicates that ALL options in the list are included in the report.

Option	Description
Creation Start and End Date(s)	The access review creation date range. The report includes all access reviews create on or after the start date and on or before the end date. You can enter the date manually, or click the **"..."** icon to select a date from the calendar.
Signed Start and End Date (s)	The access review signed off on date range. The report includes all access reviews signed off on, on or after the start date and on or before the end date. You can enter the date manually, or click the **"..."** icon to select a date from the calendar.
Due Start and End Date(s)	The access review due date range. The report includes all access reviews due on or after the start date and on or before the end date. You can enter the date manually, or click the **"..."** icon to select a date from the calendar.
Roles	The roles to include in the report. If no roles are specified, all roles are included. Click the arrow to the right of the suggestion field to display a list of all roles, or enter a few letters in the field to display a list of roles that start with that letter string.
Certification Tags	To filter access reviews based on their tags, select one or more tags. If multiple tags are selected, only access reviews that match all selected tags are included in this report.
Certification Group	The type of role certifications to include in this report; Membership or Composition.
Show excluded items	Show items that were excluded from the certification through a rule or other criteria. **Note: This option disables the preview grid view and the option to sort by Status, Decision, Decision Maker, Application, or Recommendation.**

Role Membership Access Review Live Report

This report includes information about all Role Membership Access Reviews in IdentityIQ. The Role Membership Access Review certifies that roles for which the reviewer is responsible are assigned to the correct identities. The report's purpose is to show the decisions made on each item, along with the decision maker's name and comments and the current status of any applicable revocations.

This report includes information in the detailed results format that can be exported to a .csv file and used as spreadsheets.

The Role Membership Access Review Report consists of the following sections:

- Standard Report Properties
- Certification Properties. These are described in the table below.
- Report Layout

All reports use a set of standard properties for basic information, such as naming and descriptions, and to set controls, such as scope and to required sign off.

You must enter the following before running this report:

- Name
- Role

For step by step instructions on creating or editing a report, see Working With Reports

Certification Properties

The following criteria determines what information is included in this report. You can use any combination of options to build a report.

> Selecting NO options from a list indicates that ALL options in the list are included in the report.

Option	Description
Creation Start and End Date(s)	The access review creation date range. The report includes all access reviews create on or after the start date and on or before the end date. You can enter the date manually, or click the **"..."** icon to select a date from the calendar.
Signed Start and End Date (s)	The access review signed off on date range. The report includes all access reviews signed off on, on or after the start date and on or before the end date. You can enter the date manually, or click the **"..."** icon to select a date from the calendar.
Due Start and End Date(s)	The access review due date range. The report includes all access reviews due on or after the start date and on or before the end date. You can enter the date manually, or click the **"..."** icon to select a date from the calendar.
Roles	The roles to include in the report. If no roles are specified, all roles are included. Click the arrow to the right of the suggestion field to display a list of all roles, or

Option	Description
	enter a few letters in the field to display a list of roles that start with that letter string.
Certification Tags	To filter access reviews based on their tags, select one or more tags. If multiple tags are selected, only access reviews that match all selected tags are included in this report.
Certification Group	The type of role certifications to include in this report; Membership or Composition.
Show excluded items	Show items that were excluded from the certification through a rule or other criteria. **Note: This option disables the preview grid view and the option to sort by Status, Decision, Decision Maker, Application, or Recommendation.**

Targeted Access Review Live Report

The Targeted Access Review Live Report includes information about all targeted access reviews in IdentityIQ.

This report includes information in the detailed results format that can be exported to a .csv file and used as spreadsheets.

The Targeted Access Review Live Report consists of the following sections:

- Standard Report Properties
- Certification Properties. These are described in the table below.
- Report Layout

All reports use a set of standard properties for basic information, such as naming and descriptions, and to set controls, such as scope and to required sign off.

You must enter the following before running this report:

- Name

For step by step instructions on creating or editing a report, see Working With Reports

Certification Properties

The following criteria determines what information is included in this report. You can use any combination of options to build a report.

> Selecting NO options from a list indicates that ALL options in the list are included in the report.

Option	Description
Creation Start and End Date(s)	The access review creation date range. The report includes all access reviews create on or after the start date and on or before the end date. You can enter the date manually, or click the **"..."** icon to select a date from the

Option	Description
	calendar.
Signed Start and End Date (s)	The access review signed off on date range. The report includes all access reviews signed off on, on or after the start date and on or before the end date. You can enter the date manually, or click the **"..."** icon to select a date from the calendar.
Due Start and End Date(s)	The access review due date range. The report includes all access reviews due on or after the start date and on or before the end date. You can enter the date manually, or click the **"..."** icon to select a date from the calendar.
Certification Tags	To filter access reviews based on their tags, select one or more tags. If multiple tags are selected, only access reviews that match all selected tags are included in this report.
Certification Group	The type of role certifications to include in this report; Membership or Composition.

Account Group Reports

- Account Group Members Report
- Account Group Membership Totals Report

Account Group Members Report

The Account Group Members Report includes information about all the members of all the account groups and application objects. You can filter this report to include only account groups on a specific application or set of applications.

This report includes information in the detailed results format that can be exported to a .csv file and used as spreadsheets.

The Account Group Members Report consists of the following sections:

- Standard Report Properties
- Report Options. These options are described in the Report Options table below.
- Report Layout

All reports use a set of standard properties for basic information, such as naming and descriptions, and to set controls, such as scope and to required sign off.

You must enter the following before running this report:

- Name
- Application

For step by step instructions on creating or editing a report, see Working With Reports

Report Options

The following criteria determines what information is included in this report. You can use any combination of options to build a report.

> Selecting NO options from a list indicates that ALL options in the list are included in the report.

Option	Description
Application	Select which application(s) to include in the report.

Account Group Membership Totals Report

The Account Group Membership report lists all account groups for the selected application(s), and shows the count of account group members for each. This report can be filtered to include only account groups on a specific application or set of applications. If no applications are specified as filters, account groups for all applications are included on the report.

This report includes information in the detailed results format that can be exported to a .csv file and used as spread-sheets.

The Account Group Membership Report consists of the following sections:

- Standard Report Properties
- Report Options. These options are described in the Report Options table below.
- Report Layout

All reports use a set of standard properties for basic information, such as naming and descriptions, and to set controls, such as scope and to required sign off.

You must enter the following before running this report:

- Name
- Application
- Member Options

For step by step instructions on creating or editing a report, see Working With Reports

Report Options

The following criteria determines what information is included in this report. You can use any combination of options to build a report.

> Selecting NO options from a list indicates that ALL options in the list are included in the report.

Option	Description
Application	Select which application(s) to include in the report.

Activity Reports: User Activity Detailed Report

The User Activity Detailed Report includes information on all activity on the applications monitored by IdentityIQ according to the criteria specified. This report is only applicable if activity monitoring has been configured in the system See the **Application Configuration** documentation for more information.

This report includes information in the detailed results format that can be exported to a .csv file and used as spreadsheets.

The User Activity Report consists of the following sections:

- Standard Report Properties
- Additional Identity Properties. These options are described in the table below.
- Report Layout

All reports use a set of standard properties for basic information, such as naming and descriptions, and to set controls, such as scope and to required sign off.

You must enter the following before running this report:

- Name

For step by step instructions on creating or editing a report, see Working With Reports

Additional Identity Properties

The following criteria determines what information is included in this report. You can use any combination of options to build a report.

> Selecting NO options from a list indicates that ALL options in the list are included in the report.

Option	Description
Identities	The identity list to include in this report. If no identities are specified, activity for all identities is included. Click the arrow to the right of the suggestion field to display a list of all identities, or enter a few letters in the field to display a list of identities that start with that letter string.
Applications	Select the applications to include in the report. If no applications are specified, all applications configured to track activity are included. Click the arrow to the right of the suggestion field to display a list of all applications, or enter a few letters in the field to display a list of applications that start with that letter string.
Start and End Dates	The first and last date for which activity is reported. The report includes all application activity that occurred within the date range specified. You can enter the date manually, or click the **"..."** icon to select a date from the calendar.
Action	The actions to include in the report. Only activity of the action types selected are included in the report. Use the Ctrl and Shift keys to select multiple actions.
Result	The activity results to include in the report. Only activities that include the selected result, Success or Failure, are included.
Target	The specific target on an application to include in the report. Use the target filter to further narrow the result set for a search on a specific application.

Administration Reports

Capabilities to Identities Report

The Capabilities to Identities Report displays a list of the identities assigned to each capability defined in your enterprise.

This report includes information in the detailed results format that can be exported to a .csv file and used as spreadsheets.

The Capabilities to Identities Report consists of the following sections:

- Standard Report Properties
- Capability Properties. These options are described in the table below.
- Report Layout

All reports use a set of standard properties for basic information, such as naming and descriptions, and to set controls, such as scope and to required sign off.

You must enter the following before running this report:

- Name

For step by step instructions on creating or editing a report, see Working With Reports

Capabilities Properties

The following criteria determines what information is included in this report. You can use any combination of options to build a report.

> Selecting NO options from a list indicates that ALL options in the list are included in the report.

Option	Description
Capabilities	The capabilities to include in the report.
Exclude Indirect Capabilities	Do not include identities that have the capability assigned indirectly, through a workgroup.
Exclude Workgroups	Do not include workgroups in the report results.

Connectivity Information Report

The Connectivity Information Report displays all of the information collected about application configurations and statistics that match the specified criteria.

This report collects the following information:

- Application configuration attributes and schema from Application xml.
- Last aggregation run time for all type of aggregations such as, Account aggregation, Group aggregation, and Delta aggregation.
- Average time taken for all type of aggregations.
- Schedule frequency for all type of aggregations.
- Provisioning operations statistics such as, number of create, update, and change password.
- Total accounts and groups.
- Maximum and average entitlements per account.
- Maximum and average members per group.

> Remove sensitive data before exporting.

This report includes information in the detailed results format that can be exported to a .csv file and used as spreadsheets.

The Connectivity Information Report consists of the following sections:

- Standard Report Properties
- Application Filter
- Attributes Filter
- Report Layout

All reports use a set of standard properties for basic information, such as naming and descriptions, and to set controls, such as scope and to required sign off.

You must enter the following before running this report:

- Name

For step by step instructions on creating or editing a report, see Working With Reports

Application Filter

Specify applications to exclude from this report. You can exclude applications by type or name. For excluded application, only statistical information is collected. Application configuration details are ignored for excluded applications.

Attribute Filter

Specify attributes to exclude from this report. The values of the application attributes displayed in the list are not included in the report.

Detailed Provisioning Transaction Object Report

The Detailed Provisioning Transaction Object Report displays information reflected in the Administrator Console's Provisioning Transactions table, down to the attribute level of detail. In the Administrator Console UI page (**Gear menu > Administrator Console**), clicking the information button on a given transaction displays these details for that individual line item. This report displays the data in a report format, across multiple transactions at once. For more information on the Provisioning Transaction Table, see the **System Administration** documentation.

This report includes information in the detailed results format that can be exported to a .csv file and used as spreadsheets.

The Detailed Provisioning Transaction Object Report consists of the following sections:

- Standard Report Properties
- Provisioning Transaction Properties. These options are described in the table below.
- Report Layout

All reports use a set of standard properties for basic information, such as naming and descriptions, and to set controls, such as scope and to required sign off.

You must enter the following before running this report:

- Name

For step by step instructions on creating or editing a report, see Working With Reports

Provisioning Transaction Properties

The following criteria determines what information is included in this report. You can use any combination of options to build a report.

> Selecting NO options from a list indicates that ALL options in the list are included in the report.

Option	Description
Application	The applications list to include in this report. Click the arrow to the right of the suggestion field to display a list of all applications, or enter a few letters in the field to display a list of applications that start with that letter string.
Identities	The identities list to include in this report. Click the arrow to the right of the suggestion field to display a list of all identities, or enter a few letters in the field to display a list of identities that start with that letter string.
Channel	Include provisioning transactions which have been processed through one of the specified write channels (e.g. connector or integration). Click the arrow to the right of the suggestion field to display a list of all available channels, or enter a few letters in the field to display a list of channels that start with that letter string.
Account	Limit returned provisioning transactions to those with the account display name begins with value entered in this field.
Event	The events list to include in this report (such as Create, Modify, Disable, etc.) Click the arrow to the right of the suggestion field to display a list of all available events, or enter a few letters in the field to display a list of events that start with that letter string.
Source	The source list to include in this report. Click the arrow to the right of the suggestion field to display a list of all available sources, or enter a few letters in the field to display a list of sources that start with that letter string.
Status	The status list to include in this report, such as Failed, Success, or Pending.

Option	Description
	Click the arrow to the right of the suggestion field to display a list of all available statuses, or enter a few letters in the field to display a list of statuses that start with that letter string.
Type	Select Manual or Auto to limit the results of this report by transaction type. **Auto** means the original provisioning request was (or is being) processed by a connector or integration. **Manual** means a manual work item was created to manage the provisioning request because the target application is not connected to an automated write channel.
Transaction Initiation Date	Limit the report results by date range.
Overridden	Include only transactions which have previously failed but have been overridden by creating a manual work item to have it processed outside of IdentityIQ's automated provisioning channels; once a transaction has failed with a non-retryable error, a manual work item is the only option for processing the provisioning request through a channel IdentityIQ will track

Environment Information Report

The Environment Information Report gives detailed information about user activity on each application. Count statistics are provided for a number of IdentityIQ objects: identities, applications, accounts, work items, identity requests, workgroups, certifications, task schedules, roles, policies, and entitlement catalog. Note that for these objects the value column shows **counts** of objects. Individual identity data is not included in this report, to ensure that privacy requirements are met if the report needs to be shared.

The Environment Information Report also shows information about your IdentityIQ environment, such as database type, version and driver, JDBC drivers and hosts, processor details, and IdentityIQ version:

The Environment Information Report consists of the following sections:

- Standard Report Properties
- Report Layout

All reports use a set of standard properties for basic information, such as naming and descriptions, and to set controls, such as scope and to required sign off.

There are no filter options for this report. It always reports the full set of environment data. You must enter the following before running this report:

- Name

For step by step instructions on creating or editing a report, see Working With Reports

Identity to Capabilities Report

The Identity to Capabilities Report displays a list of the capabilities assigned to each identity in your enterprise.

This report includes information in the detailed results format that can be exported to a .csv file and used as spreadsheets.

The Capabilities to Identities Report consists of the following sections:

- Standard Report Properties
- Identity Properties. These are described in the table below.
- Report Layout

All reports use a set of standard properties for basic information, such as naming and descriptions, and to set controls, such as scope and to required sign off.

You must enter the following before running this report:

- Name

For step by step instructions on creating or editing a report, see Working With Reports

Identity Properties

The following criteria determines what information is included in this report. You can use any combination of options to build a report.

> Selecting NO options from a list indicates that ALL options in the list are included in the report.

Option	Description
Identities	The identities to include in the report.
Include Empty Capabilities	Include identities that have no assigned capabilities.
Exclude Indirect Capabilities	Do not include capabilities assigned through workgroups in the report results.
Exclude Workgroups	Do not include workgroups in the report results.

Mitigation Report

This report lists policy exceptions that have been allowed in the system. It can be used to review the mitigation decisions made by a given actor, to see the exceptions allowed for certain people or against certain roles, or to review exceptions that are set to expire by a given date.

This report includes information in the detailed results format that can be exported to a .csv file and used as spreadsheets.

The Mitigation Report consists of the following sections:

- Standard Report Properties
- Mitigation Properties. These are described in the table below.
- Report Layout

All reports use a set of standard properties for basic information, such as naming and descriptions, and to set controls, such as scope and to required sign off.

You must enter the following before running this report:

- Name

For step by step instructions on creating or editing a report, see Working With Reports

Mitigation Properties

The following criteria determines what information is included in this report. You can use any combination of options to build a report.

> Selecting NO options from a list indicates that ALL options in the list are included in the report.

Option	Description
Expiration Date	The expiration limit on the exception. Exceptions that expire on dates up to and including the selected date are included in this report. You can enter the date manually, or click the **"..."** icon to select a date from the calendar.
Identities	The identities list to include in this report. If no identities are specified, mitigation for all identities are included. Click the arrow to the right of the suggestion field to display a list of all identities, or enter a few letters in the field to display a list of identities that start with that letter string.
Actors	The manager (mitigator) list to include in this report. If no managers are specified, mitigations for all managers are included. Click the arrow to the right of the suggestion field to display a list of all managers, or enter a few letters in the field to display a list of managers that start with that letter string.
Business Roles	The roles list to include in this report. If no roles are specified, mitigation on all roles are included. Click the arrow to the right of the suggestion field to display a list of all roles, or enter a few letters in the field to display a list of roles that start with that letter string.

Provisioning Transaction Object Report

The Provisioning Transaction Object Report shows data reflected in the Administrator Console's Provisioning Transactions table. This report captures the summary level of transaction data, which is the same level of information displayed in the Provisioning Transaction table in the UI. . For more information on the Provisioning Transaction Table, see the **System Administration** documentation.

The Provisioning Transaction Object Report consists of the following sections:

- Standard Report Properties
- Provisioning Transaction Properties. These are described in the table below.
- Report Layout

All reports use a set of standard properties for basic information, such as naming and descriptions, and to set controls, such as scope and to required sign off.

You must enter the following before running this report:

- Name

For step by step instructions on creating or editing a report, see Working With Reports

Provisioning Transaction Properties

The following criteria determines what information is included in this report. You can use any combination of options to build a report.

> Selecting NO options from a list indicates that ALL options in the list are included in the report.

Option	Description
Application	Shows only provisioning transactions which impact one of the specified applications. Click the arrow to the right of the suggestion field to display a list of all applications, or enter a few letters in the field to display a list of applications that start with that letter string.
Identities	The identities list to include in this report. Click the arrow to the right of the suggestion field to display a list of all identities, or enter a few letters in the field to display a list of identities that start with that letter string.
Channel	The channels list to include in this report. Click the arrow to the right of the suggestion field to display a list of all available channels, or enter a few letters in the field to display a list of channels that start with that letter string.
Account	Limit returned provisioning transactions to those with the account display name begins with value entered in this field.
Event	The events to include in this report, such as Create, Modify, Disable, etc. Click the arrow to the right of the suggestion field to display a list of all available events, or enter a few letters in the field to display a list of events that start with that letter string.
Source	List only transactions which came from one of the selected sources in IdentityIQ (e.g. LCM, Identity Refresh, etc.). Click the arrow to the right of the suggestion field to display a list of all available sources, or enter a few letters in the field to display a list of sources that start with that letter string.
Status	The status list to include in this report. Click the arrow to the right of the suggestion field to display a list of all available statuses, or enter a few letters in the field to display a list of statuses that start with that letter string.
Type	Select Manual or Auto to limit the results of this report by transaction type. **Auto** means the original provisioning request was (or is being) processed by a connector or integration. **Manual** means a manual work item was created to manage the provisioning request because the target application is not connected to an automated write channel.

Option	Description
Transaction Initiation Date	Limit the report results by date range.
Overridden	Include only transactions which have previously failed but have been overridden by creating a manual work item to have it processed outside of IdentityIQ's automated provisioning channels (once a transaction has failed with a non-retryable error, a manual work item is the only option for processing the provisioning request through a channel IdentityIQ will track)

Revocation Live Report

This report shows all access revocation requests made in access reviews which meet the filter criteria and the current status of the revocation (open or finished). It also shows information about the revocation request such as who requested it, how the request was (or is being) revoked, the name of the person processing the revoke (for work item revocations only), the access request ID (for queued automated requests on some systems), the Identity from whom the access has been revoked, and any comments entered by the requester. It also includes the expiration date of the certification in which it was revoked, along with identifying information about which specific entitlement or role was revoked.

This report includes information in the detailed results format that can be exported to a .csv file and used as spreadsheets.

The Revocation Live Report consists of the following sections:

- Standard Report Properties
- Certification Item Properties. These are described in the table below.
- Report Layout

You must enter the following before running this report:

- Name

For step by step instructions on creating or editing a report, see Working With Reports

Certification Items Properties

The following criteria determines what information is included in this report. You can use any combination of options to build a report.

> Selecting NO options from a list indicates that ALL options in the list are included in the report.

Option	Description
Creation Start and End Date (s)	The certification creation date range. The report includes all revocation information for certifications create on or after the start date and on or before the end date. You can enter the date manually, or click the **"..."** icon to select a date from the calendar.

Option	Description
Signed Start and End Date (s)	The certification signed off on date range. The report includes all revocation information for certifications signed off on, on or after the start date and on or before the end date. You can enter the date manually, or click the **"..."** icon to select a date from the calendar.
Due Start and End Date(s)	The certification due date range. The report includes all revocation information for certifications due on or after the start date and on or before the end date. You can enter the date manually, or click the **"..."** icon to select a date from the calendar.
Applications	Select the applications to include in the report. If no applications are specified, all applications are included. Click the arrow to the right of the suggestion field to display a list of all applications, or enter a few letters in the field to display a list of applications that start with that letter string.
Group	Select the groups to include in this report. Click the arrow to the right of the suggestion field to display a list of all groups, or enter a few letters in the field to display a list of groups that start with that letter string.
Certification Tags	To filter access reviews based on their tags, select one or more tags. If multiple tags are selected, only access reviews that match all selected tags are included in this report.
Certification Group	The manager certifications to include in this report.

Work Item Archive Report

This report shows the current status of work items in the system. It can report on active work items, archived work items or both (depending on the Included Work Items filter). It shows the requester, work item owner, type, current state, number of reminders and escalations that have occurred for it, and its current status.

This report includes information in the detailed results format that can be exported to a .csv file and used as spreadsheets.

The Work Item Archive Report consists of the following sections:

- Standard Report Properties
- Work Item Properties. These are described in the table below.
- Report Layout

All reports use a set of standard properties for basic information, such as naming and descriptions, and to set controls, such as scope and to required sign off.

You must enter the following before running this report:

- Name

For step by step instructions on creating or editing a report, see Working With Reports

Work Item Properties

The following criteria determines what information is included in this report. You can use any combination of options to build a report.

> Selecting NO options from a list indicates that ALL options in the list are included in the report.

Option	Description
Owners	The owners of the work items. Only work items belonging to the selected owners are included in the report. Click the arrow to the right of the suggestion field to display a list of all owners, or enter a few letters in the field to display a list of owners that start with that letter string.
Requestors	The requestors of the work items. Only work items requested by the selected requestors are included in the report. Click the arrow to the right of the suggestion field to display a list of all requestors, or enter a few letters in the field to display a list of requestors that start with that letter string.
Work Items Priority	The priority assigned by the requestor of the work item.
Work Items Type	The work item types to include in this report. Only work items of the type selected are included in the report. Use the Shift and Ctrl buttons to select multiple types.
Work Item State	The state of the work items to include in this report. Only work items in the selected states are included in the report. Use the Shift and Ctrl buttons to select multiple states.
Included Work Items	Choose to include active or archived work items in the report.
Minimum Reminders	The minimum number of sent reminders that a work item must be associate with before it is included in this report.
Maximum Reminders	The maximum number of sent reminders that a work item can be associated with and still be included in this report.

Application Status Report

This report shows statistics about managed applications defined in the system. Specifically, it shows the number of accounts aggregated, the last aggregation date, the earliest and latest last refresh dates marked on any account for the application (useful for partial or delta aggregations), the total count of entitlements held on the application (Total Assignments), and the count of unique entitlements (distinct attribute name-value-type combination) existing on the application.

This report includes information in the detailed results format that can be exported to Microsoft Excel and used as spreadsheets.

The Application Status Report consists of the following sections:

- Standard Report Properties
- Report Options. These options are described in the table below.
- Report Layout

All reports use a set of standard properties for basic information, such as naming and descriptions, and to set controls, such as scope and to required sign off.

You must assign a name before running this report:

For step by step instructions on creating or editing a report, see Working With Reports

Report Options

The following criteria determines what information is included in this report. You can use any combination of options to build a report.

- Applications: Select the applications to include in the report. Click the arrow to the right of the suggestion field to display a list of all applications, or enter a few letters in the field to display a list of applications that start with that letter string.

> Selecting NO options from a list indicates that ALL options in the list are included in the report.

Report Data

The Application Status Report displays the following data:

- Application
- Number of Accounts
- Last Aggregation
- Oldest Refresh Time
- Newest Refresh Time
- Total Assignments
- Unique Entitlements

Configured Resource Reports

- Configured Applications Archive Report
- Configured Applications Detail Report
- Delimited File Application Status Report

Configured Applications Archive Report

This report shows key attributes of all applications meeting specified report filters. Specifically, it indicates the connector in use, the owner, the object types defined (account, group), and the identity attribute and display attribute selected for each object schema. It also shows the application's creation date and last updated date. Finally, the IdentityIQ Authentication attribute indicates whether the application is used for pass-through-authentication to authenticate users to IdentityIQ.

This report is an archive-type report. Archive reports include end-of-period and task information that is formatted for easy dissemination of key audit information.Due to the large amount of data that is generated, the best option is to export the report results to a .pdf file.

All reports use a set of standard properties for basic information, such as naming and descriptions, and to set controls, such as scope and to required sign off.

You must enter the following before running this report:

- Name

For more information on Standard Properties, see Standard Report Properties

For more information on Report Layout, see Report Layout

For step by step instructions on creating or editing a report, see Working With Reports

Application Properties

The following criteria determines what information is included in this report. You can use any combination of options to build a report.

> Selecting NO options from a list indicates that ALL options in the list are included in the report.

Option	Description
Applications	Select the applications to include in the report. If no applications are specified, all applications are included. Click the arrow to the right of the suggestion field to display a list of all applications, or enter a few letters in the field to display a list of applications that start with that letter string.
Owners	The application owners to include in the report. Only applications associated with selected application owners are included in the report Click the arrow to the right of the suggestion field to display a list of all owners, or enter a few letters in the field to display a list of owners that start with that letter string.

Configured Applications Detail Report

This report shows the name, connector type, owner, and revoker specified for each application configured in the system.

This report includes information in the detailed results format that can be exported to a .csv file and used as spreadsheets.

The Configured Applications Detail Report consists of the following sections:

- Standard Report Properties
- Application Properties. These options are described in the table below.
- Report Layout

All reports use a set of standard properties for basic information, such as naming and descriptions, and to set controls, such as scope and to required sign off.

You must enter the following before running this report:

- Name

For step by step instructions on creating or editing a report, see Working With Reports

Application Properties

The following criteria determines what information is included in this report. You can use any combination of options to build a report.

> Selecting NO options from a list indicates that ALL options in the list are included in the report.

Option	Description
Applications	Select the applications to include in the report. If no applications are specified, all applications are included. Click the arrow to the right of the suggestion field to display a list of all applications, or enter a few letters in the field to display a list of applications that start with that letter string.
Owners	The application owners to include in the report. Only applications associated with selected application owners are included in the report Click the arrow to the right of the suggestion field to display a list of all owners, or enter a few letters in the field to display a list of owners that start with that letter string.

Delimited File Application Status Report

The Delimited File Application Status Report includes information about applications that are of type Delimited File Parsing Connector and that also have local file types. For example, applications that use delimited files, but are acquired through a proxy such as ftp are not shown in the report.

Specifically, the report indicates the last time the application was aggregated and statistics about the file to which it is pointed, including file name, date, size, and calculated file age. The report does not include information on the end date of that aggregation or if it was successful. Therefore this report should not be used as an indicator of application aggregation success.

This report includes information in the detailed results format that can be exported to a .csv file and used as spreadsheets.

The Delimited File Application Status Report consists of the following sections:

- Standard Report Properties
- Delimited File Properties. These options are described in the table below.
- Report Layout

All reports use a set of standard properties for basic information, such as naming and descriptions, and to set controls, such as scope and to required sign off.

You must enter the following before running this report:

- Name

For step by step instructions on creating or editing a report, see Working With Reports

Delimited File Properties

The following criteria determines what information is included in this report. You can use any combination of options to build a report.

> Selecting NO options from a list indicates that ALL options in the list are included in the report.

Option	Description
Application	Select which application to include in the report.

Identity and User Reports

- Account Attributes Live Report
- Application Account Summary Report
- Application Account by Attribute Report
- Identity Effective Access Live Report
- Identity Entitlements Detail Report
- Identity Forwarding Report
- Identity Status Summary Report
- Privileged Access Report
- Uncorrelated Accounts Report
- User Account Attributes Report
- User Security Question Status Report
- User Details Report
- Users by Application Report

Account Attributes Live Report

This report shows the account attributes for every application account held by every identity (according to filters applied). Each account attribute and value combination is listed on a separate line of the report results.

This report can be filtered to include accounts for a subset of identities based on values specified for core identity attributes, extended identity attributes, and other extended properties of identities such as the capabilities assigned to them and the groups to which they belong. If one or more applications are selected, only accounts on those applications are included in the report.

This report includes information in the detailed results format that can be exported to a .csv file and used as spreadsheets.

The Account Attributes Live Report consists of the following sections:

- Standard Report Properties
- Identity Attributes
- Identity Properties
- Report Layout

> Based on how IdentityIQ was set up for your enterprise, other attributes may be available. Extended attributes may include items such as region, location, department, and other attributes specific to your deployment.

All reports use a set of standard properties for basic information, such as naming and descriptions, and to set controls, such as scope and to required sign off.

You must enter the following before running this report:

- Name

For step by step instructions on creating or editing a report, see Working With Reports

Identity Attributes

The following criteria determines what information is included in this report. You can use any combination of options to build a report.

> Selecting NO options from a list indicates that ALL options in the list are included in the report.

> Use the Shift and Crtl keys to select multiple items from lists.

Option	Description
User Attributes	The user attributes on which to filter. Only users with the listed attributes are included in the report. This information is discovered during identity aggregation. Identity attributes can be configured. The attributes that display can vary for each instance of the product.
First Name	Input the first name of the identity you wish the report to include. For example, if you input “John” in the field, the report includes information on identities whose first name is John.
Last Name	Input the last name of the identity you wish the report to include. For example, if you input “Smith” in the field, the report includes information on identities whose last name is Smith.
Display Name	Input the display name of the identity you wish the report to include. For example, if you input “John_Smith” in the field, the report includes information on identities whose display name is John_Smith.
Email	Input the email address of the identity you wish the report to include. For example, if you input “John@email.com” in the field, the report includes information on identities whose email address is name is John@email.com.
Manager	The manager list to include in this report. Only users who report to the selected managers are included in the report. Click the arrow to the right of the suggestion field to a list of all managers, or enter a few letters in the field to display a list of managers that start with that letter string.
Inactive	Choose how the report handles inactive users. Select **No selection** to include both inactive and active users, **True** to include only inactive users, or **False** to not include inactive users.

Identity Properties

The following criteria determines what information is included in this report. You can use any combination of options to build a report.

> Selecting NO options from a list indicates that ALL options in the list are included in the report.

> Use the Shift and Crtl keys to select multiple items from lists.

Option	Description
Applications	Select the applications to include in the report. If no applications are specified, all applications are included. Click the arrow to the right of the suggestion field to display a list of all applications, or enter a few letters in the field to display a list of applications that start with that letter string.
Capabilities	Select the capabilities to include in the report.
Groups	The groups or populations to include in the report. Click the arrow to the right of the field and select a group to create the inclusion list for this report.
Last Refresh Date	Select a date range to filter users based on when the user was last refreshed.
Last Login Date	Specify a login date range manually or click the calendar icon and select one using the calendar options.
Show authorized scopes and capabilities	Select this option to include authorized scopes and capabilities for each identity in the report.

Application Account Summary Report

This report shows counts of the number of accounts on each application, the number of identities with accounts on each application, and the number of identities with more than one account on each application.

This report includes information in the detailed results format that can be exported to a .csv file and used as spreadsheets.

The Application Account Summary Report consists of the following sections:

- Standard Report Properties
- Report Options. These options are described in the table below.
- Report Layout

All reports use a set of standard properties for basic information, such as naming and descriptions, and to set controls, such as scope and to required sign off.

You must enter the following before running this report:

- Name

For step by step instructions on creating or editing a report, see Working With Reports

Report Options

The following criteria determines what information is included in this report.

Option	Description
Applications	Select the applications to include in the report. If no applications are specified, all applications are included. Click the arrow to the right of the suggestion field to display a list of all applications, or enter a few letters in the field to display a list of applications that start with that letter string.

Selecting NO options from a list indicates that ALL options in the list are included in the report.

Use the Shift and Crtl keys to select multiple items from lists.

Application Account by Attribute Report

This report shows each account aggregated from the selected application and the Identity to which each account is linked. This report can be run for only one application at a time, so the Application filter is required. Other filters are determined by the configured extended account attributes for the installation. Boolean attributes offer the option to select either value or none (to include accounts with either value set); date attributes can be constrained by a start or end date or both. String attributes are analyzed for an exact match to the entered filter value.

This report includes information in the detailed results format that can be exported to a .csv file and used as spreadsheets.

The Application Account by Attribute Report consists of the following sections:

- Standard Report Properties
- Account Properties. These options are described in the table below.
- Report Layout

All reports use a set of standard properties for basic information, such as naming and descriptions, and to set controls, such as scope and to required sign off.

You must enter the following before running this report:

- Name

For step by step instructions on creating or editing a report, see Working With Reports

Account Properties

The following criteria determines what information is included in this report. You can use any combination of options to build a report.

Selecting NO options from a list indicates that ALL options in the list are included in the report.

Option	Description
Applications	Select the applications to include in the report. If no applications are specified, all applications are included. Click the arrow to the right of the suggestion field to display a list of all applications, or enter a few letters in the field to display a list of applications that start with that letter string.
Inactive Account	Choose how the report handles inactive accounts. Select **No selection** to include both inactive and active accounts, **True** to include only inactive accounts, or **False** to not include inactive accounts.
Privileged Account	Choose how the report handles privileged accounts. Select **No selection** to include both privileged and standard accounts, **True** to include only privileged accounts, or **False** to not include privileged accounts.
Service Account	Choose how the report handles service accounts. Select **No selection** to include both service and standard accounts, **True** to include only service accounts, or **False** to not include service accounts.
Last login	Specify a login date range manually or click the calendar icon and select one using the calendar options.

Identity Effective Access Live Report

This report lists all entitlements, including account group memberships, found for identities meeting the filter criteria specified. When an entitlement is encapsulated in a detected role and/or is granted to the user based on an assigned role, the associated roles are also shown on the report row for that entitlement.

This report can be filtered to include entitlements for a subset of identities based on values specified for core identity attributes, extended identity attributes, and extended properties of identities such as the capabilities assigned to them, and the groups to which they belong. If one or more applications are selected, only accounts on those applications are included in the report.

This report includes information in the detailed results format that can be exported to a .csv file and used as spreadsheets.

The Identity Effective Access Live Report consists of the following sections:

- Standard Report Properties
- Identity Attributes
- Identity Extended Attributes
- Additional Identity Properties
- Report Layout

All reports use a set of standard properties for basic information, such as naming and descriptions, and to set controls, such as scope and to required sign off.

You must enter the following before running this report:

- Name

For step by step instructions on creating or editing a report, see Working With Reports

Identity Attributes

The following criteria determines what information is included in this report. You can use any combination of options to build a report.

Option	Description
First Name	Input the first name of the identity you wish the report to include. For example, if you input “John” in the field, the report includes information on identities whose first name is John.
Last Name	Input the last name of the identity you wish the report to include. For example, if you input “Smith” in the field, the report includes information on identities whose last name is Smith.
Display Name	Input the display name of the identity you wish the report to include. For example, if you input “John_Smith” in the field, the report includes information on identities whose display name is John_Smith.
Email	Input the email address of the identity you wish the report to include. For example, if you input “John@email.com” in the field, the report includes information on identities whose email address is name is John@email.com.
Manager	The manager list to include in this report. Only users who report to the selected managers are included in the report. Click the arrow to the right of the suggestion field to a list of all managers, or enter a few letters in the field to display a list of managers that start with that letter string.
Inactive	Choose how the report handles inactive identities. Select **No selection** to include both inactive and active identities, **True** to include only inactive identities, or **False** to not include inactive identities.

Identity Extended Attributes

You can use the identity extended attributes that have been defined for your installation as criteria for this report. Because these are custom-defined attributes, the specific criteria options you have here will be specific to your own installation of IdentityIQ. Any identity extended attributes **defined as searchable or as multi-valued** are included as possible filters for the report.

Additional Identity Properties

The following criteria determines what information is included in this report. You can use any combination of options to build a report.

Option	Description
Applications	Select the applications to include in the report. If no applications are specified, all applications are included. Click the arrow to the right of the suggestion field to display a list of all applications, or enter a few letters in the field to display a list of applications that start with that letter string.

Option	Description
Capabilities	Select the capabilities to include in the report.
Roles	The roles to include in the report. Click the arrow to the right of the field and select a role to create the inclusion list for this report.
Groups	The groups or populations to include in the report. Click the arrow to the right of the field and select a group to create the inclusion list for this report.
Last Refresh Date	Select a date range to filter users based on when the user was last refreshed.
Last Login Date	Select a date range to filter users based on when the user was last logged in.

Identity Entitlements Detail Report

> Including classifications in the Identity Entitlements Detail Report can impact performance. By default, classifications are included in this report, but you can remove them in the Report Layout dialog.

This report lists all identity entitlements – assigned and aggregated application entitlements, assigned and detected roles – and details about them. Some columns apply only to application entitlements, some apply only to roles, and some relate to both.

- For **application entitlements**, the data displayed includes the application name and instance (if applicable), the attribute name and value, the account name, and whether it was directly assigned (e.g. requested through LCM) or whether it was granted indirectly by one or more of the Identity's roles.
- For **roles**, the Attribute columns shows whether it was assigned or detected, and the Entitlement column shows the role name; the Allowed column is only ever "true" for detected roles which are allowed or required by an assigned role for the Identity.

Information about when they were last certified for the identity is shown for both types of records, as is the Source data (how the entitlement/role was granted to or found for the identity).

This report includes information in the detailed results format that can be exported to a .csv file and used as spreadsheets.

The Identity Entitlements Detail Report consists of the following sections:

- Standard Report Properties
- Identity Entitlements Report Arguments. These options are described in the table below.
- Report Layout

All reports use a set of standard properties for basic information, such as naming and descriptions, and to set controls, such as scope and to required sign off.

You must enter the following before running this report:

- Name

For step by step instructions on creating or editing a report, see Working With Reports

Identity Entitlements Report Arguments

The following criteria determines what information is included in this report. You can use any combination of options to build a report.

> Selecting NO options from a list indicates that ALL options in the list are included in the report.

> Use the Shift and Crtl keys to select multiple items from lists.

Option	Description
Identities	Type in manually or use the drop-down list to select the identities to include in the report. If no identities are specified, all identities are included.
Applications	Type in manually or use the drop-down list to select the applications to include in the report. If no applications are specified, all applications are included.
Attributes	Type in manually or use the drop-down list to select the attributes to include in the report. If no attributes are specified, all attributes are included.
Entitlements	Type in manually or use the drop-down list to select the entitlements to include in the report. If no entitlements are specified, all entitlements are included.
Accounts	Type in manually or use the drop-down list to select the accounts to include in the report. If no accounts are specified, all accounts are included.
Instances	Type in manually or use the drop-down list to select the instances to include in the report. If no instances are specified, all instances are included.
Assigners	Type in manually or use the drop-down list to select the assigners to include in the report. If no assigners are specified, all assigners are included.
Source	Type in manually or use the drop-down list to select the sources to include in the report. If no sources are specified, all sources are included.
Exists on account	Select **Include All** to include all entitlements **True** to include only entitlements that were found on the last aggregation, or **False** to not include entitlements that were found on the last aggregation. The default is to include both.
Entitlement Type	Select from **Include All**, **Entitlements**, or **Permissions**.
Allowed by an assigned role	Select **Include All** to include all entitlements **True** to include only entitlements that were not granted by a role, or **False** to omit these detected roles from the report; by default, they are included alongside account entitlements and assigned roles.
Additional Entitlements only	Select **Include All** to include all entitlements **True** to include only entitlements that were allowed by an assigned role, or **False** to not include entitlements that allowed by an assigned role.
Has been cer-	Select **Include All** to include all entitlements **True** to include only entitlements

Option	Description
tified	that have been certified, or **False** to not include entitlements that have been certified.
Has pending certification	Select **Include All** to include all entitlements **True** to include only entitlements that have a pending certification, or **False** to not include entitlements that have a pending certification.
Has been requested	Select **Include All** to include all entitlements **True** to include only entitlements that have been requested, or **False** to not include entitlements that have been requested.
Has pending request	Select **Include All** to include all entitlements **True** to include only entitlements that have a pending request, or **False** to not include entitlements that have a pending request.

Identity Forwarding Report

The Identity Forwarding Report shows identities that currently have a forwarding user set to redirect IdentityIQ work items to another system user. It shows the forwarding user and the date range for which forwarding is set.

This report includes information in the detailed results format that can be exported to a .csv file and used as spreadsheets.

The Identity Forwarding Report consists of the following sections:

- Standard Report Properties
- Identity Attributes
- Identity Extended Attributes
- Additional Identity Properties
- Report Layout

All reports use a set of standard properties for basic information, such as naming and descriptions, and to set controls, such as scope and to required sign off.

You must enter the following before running this report:

- Name

For step by step instructions on creating or editing a report, see Working With Reports

Identity Attributes

The following criteria determines what information is included in this report. You can use any combination of options to build a report.

Option	Description
First Name	Input the first name of the identity you wish the report to include. For example, if you input “John” in the field, the report includes information on identities whose first name is John.
Last Name	Input the last name of the identity you wish the report to include. For example, if you input “Smith” in the field, the report includes information on identities whose last

Option	Description
	name is Smith.
Display Name	Input the display name of the identity you wish the report to include. For example, if you input “John_Smith” in the field, the report includes information on identities whose display name is John_Smith.
Email	Input the email address of the identity you wish the report to include. For example, if you input “John@email.com” in the field, the report includes information on identities whose email address is name is John@email.com.
Manager	The manager list to include in this report. Only users who report to the selected managers are included in the report. Click the arrow to the right of the suggestion field to a list of all managers, or enter a few letters in the field to display a list of managers that start with that letter string.
Inactive	Choose how the report handles inactive identities. Select **No selection** to include both inactive and active identities, **True** to include only inactive identities, or **False** to not include inactive identities.

Identity Extended Attributes

You can use the identity extended attributes that have been defined for your installation as criteria for this report. Because these are custom-defined attributes, the specific criteria options you have here will be specific to your own installation of IdentityIQ. Any identity extended attributes **defined as searchable or as multi-valued** are included as possible filters for the report.

Additional Identity Properties

The following criteria determines what information is included in this report. You can use any combination of options to build a report.

Option	Description
Applications	Select the applications to include in the report. If no applications are specified, all applications are included. Click the arrow to the right of the suggestion field to display a list of all applications, or enter a few letters in the field to display a list of applications that start with that letter string.
Capabilities	Select the capabilities to include in the report.
Roles	The roles to include in the report. Click the arrow to the right of the field and select a role to create the inclusion list for this report.
Groups	The groups or populations to include in the report. Click the arrow to the right of the field and select a group to create the inclusion list for this report.
Last Refresh	Select a date range to filter users based on when the user was last refreshed.

Option	Description
Date	
Last Login Date	Select a date range to filter users based on when the user was last logged in.

Identity Status Summary Report

This report is a simple count report that shows the number of active identities, inactive identities, and total identities defined in the system. It offers no filters.

This report includes information in the detailed results format that can be exported to a .csv file and used as spreadsheets.

All reports use a set of standard properties for basic information, such as naming and descriptions, and to set controls, such as scope and to required sign off.

You must enter the following before running this report:

- Name

For more information on Standard Properties, see Standard Report Properties

For more information on Report Layout, see Report Layout

For step by step instructions on creating or editing a report, see Working With Reports

Privileged Access Report

This report lists accounts that are marked as privileged accounts on the selected application(s), specifically the display name of those accounts. It also shows the identity to which the account is linked, the identity's manager, and the risk score assigned to the identity. This report returns a list of all accounts meeting the specified criteria. To make this function as a privileged access report, an account attribute must be defined for the installation to designate privileged accounts, and that attribute and privileged-account-designating value must be specified as a filter criterion for the report.

This report includes information in the detailed results format that can be exported to a .csv file and used as spreadsheets.

The Privileged Access Report consists of the following sections:

- Standard Report Properties
- Privileged Account Attributes
- Account Applications
- Identity Attributes
- Identity Extended Attributes
- Report Layout

All reports use a set of standard properties for basic information, such as naming and descriptions, and to set controls, such as scope and to required sign off.

You must enter the following before running this report:

- Name
- At least one Privileged Account Attribute

For step by step instructions on creating or editing a report, see Working With Reports

Privileged Account Attributes

The Privileged Account Attributes age of filter criteria shows all defined account attributes, which vary by installation. The report creator must choose the attributes and values that designate a privileged account for the system. Note that if additional account attributes are selected on this filter page, this report will be constrained to show only accounts meeting those criteria, which could make this report something other than a “privileged access” report.

> Selecting NO options from a list indicates that ALL options in the list are included in the report.

> Use the Shift and Crtl keys to select multiple items from lists.

Account Applications

> Selecting NO options from a list indicates that ALL options in the list are included in the report. Use the Shift and Crtl keys to select multiple items from lists.

Option	Description
Applications	Select the applications to include in the report. If no applications are specified, all applications are included. Click the arrow to the right of the suggestion field to display a list of all applications, or enter a few letters in the field to display a list of applications that start with that letter string.

Identity Attributes

The following criteria determines what information is included in this report. You can use any combination of options to build a report.

> Selecting NO options from a list indicates that ALL options in the list are included in the report. Use the Shift and Crtl keys to select multiple items from lists.

Option	Description
First Name	Input the first name of the identity you wish the report to include. For example, if you input “John” in the field, the report includes information on identities whose first name is John.
Last Name	Input the last name of the identity you wish the report to include. For example, if you input “Smith” in the field, the report includes information on identities whose last name is Smith.
Display	Input the display name of the identity you wish the report to include. For example, if

Option	Description
Name	you input “John_Smith” in the field, the report includes information on identities whose display name is John_Smith.
Email	Input the email address of the identity you wish the report to include. For example, if you input “John@email.com” in the field, the report includes information on identities whose email address is name is John@email.com.
Manager	The manager list to include in this report. Only users who report to the selected managers are included in the report. Click the arrow to the right of the suggestion field to a list of all managers, or enter a few letters in the field to display a list of managers that start with that letter string.
Inactive	Choose how the report handles inactive users. Select **No selection** to include both inactive and active users, **True** to include only inactive users, or **False** to not include inactive users.

Identity Extended Attributes

You can use the identity extended attributes that have been defined for your installation as criteria for this report. Because these are custom-defined attributes, the specific criteria options you have here will be specific to your own installation of IdentityIQ. Any identity extended attributes **defined as searchable or as multi-valued** are included as possible filters for the report.

Uncorrelated Accounts Report

This report shows accounts on non-authoritative applications which have not yet been correlated to authoritative identities in IdentityIQ. It can be filtered to show only accounts for selected applications or to show all uncorrelated accounts.

This report includes a summary section with a table showing the statistics of correlated identities vs. uncorrelated identities and a chart which indicates the percentage of uncorrelated accounts coming from each application in the report. These statistics and chart are based only off identities with accounts on the applications selected for the report; they do not necessarily indicate total counts in the whole system.

This report includes information in the detailed results format that can be exported to a .csv file and used as spreadsheets.

The Uncorrelated Accounts Report consists of the following sections:

- Standard Report Properties
- Uncorrelated Accounts Parameters. These are described in the table below.
- Report Layout

All reports use a set of standard properties for basic information, such as naming and descriptions, and to set controls, such as scope and to required sign off.

You must enter the following before running this report:

- Name

For step by step instructions on creating or editing a report, see Working With Reports

Uncorrelated Accounts Parameters

The following criteria determines what information is included in this report. You can use any combination of options to build a report.

> Selecting NO options from a list indicates that ALL options in the list are included in the report.

Option	Description
Correlated Applications	Select the applications to include in the report. If no applications are specified, all applications are included. Correlated Applications are applications that are to be compared with the authoritative application. Any identity that has an account on the correlated application but not on the authoritative application is considered uncorrelated. Click the arrow to the right of the suggestion field to display a list of all applications, or enter a few letters in the field to display a list of applications that start with that letter string.

User Account Attributes Report

This report shows all accounts on the selected application and the identity to which each is correlated. This report can only be run for one application at a time. If account attributes have been defined for the installation and attributes from this application's accounts have been mapped to those account attributes, they are optionally available for inclusion on the report output by selecting them on the Report Layout page.

This report includes information in the detailed results format that can be exported to a .csv file and used as spreadsheets.

The User Account Attributes Report consists of the following sections:

- Standard Report Properties
- Account Properties. These are described in the table below.
- Report Layout

All reports use a set of standard properties for basic information, such as naming and descriptions, and to set controls, such as scope and to required sign off.

You must enter the following before running this report:

- Name

For step by step instructions on creating or editing a report, see Working With Reports

Account Properties

The following criteria determines what information is included in this report. You can use any combination of options to build a report.

> Selecting NO options from a list indicates that ALL options in the list are included in the report.

Option	Description
Applications	Select the applications to include in the report. If no applications are specified, all applications are included. Click the arrow to the right of the suggestion field to display a list of all applications, or enter a few letters in the field to display a list of applications that start with that letter string.
User Inactive Status	Choose how the report handles inactive users. Select **Include All** to include both inactive and active users, **True** to include only inactive users, or **False** to not include inactive users.

User Security Question Status Report

This report shows which identities have provided answers to the authentication questions which are required to log in through the Forgot Password feature of IdentityIQ. It also shows the last login date and the manager name for each user. It can be filtered by a broad set of identity attributes and data, so it can report on subsets of identities (e.g. by manager, by department, by users with accounts on a specific application, etc.).

This report includes information in the detailed results format that can be exported to a .csv file and used as spreadsheets.

The Account Authentication Question Status Report consists of the following sections:

- Standard Report Properties
- Identity Attributes
- Identity Extended Attributes
- Additional Identity Details
- Report Layout

All reports use a set of standard properties for basic information, such as naming and descriptions, and to set controls, such as scope and to required sign off.

You must enter the following before running this report:

- Name

For step by step instructions on creating or editing a report, see Working With Reports

Identity Attributes

The following criteria determines what information is included in this report. You can use any combination of options to build a report.

Option	Description
First Name	Input the first name of the identity you wish the report to include. For example, if you input “John” in the field, the report includes information on identities whose first name is John.
Last Name	Input the last name of the identity you wish the report to include. For example, if you input “Smith” in the field, the report includes information on identities whose last

Option	Description
	name is Smith.
Display Name	Input the display name of the identity you wish the report to include. For example, if you input “John_Smith” in the field, the report includes information on identities whose display name is John_Smith.
Email	Input the email address of the identity you wish the report to include. For example, if you input “John@email.com” in the field, the report includes information on identities whose email address is name is John@email.com.
Manager	The manager list to include in this report. Only users who report to the selected managers are included in the report. Click the arrow to the right of the suggestion field to a list of all managers, or enter a few letters in the field to display a list of managers that start with that letter string.
Inactive	Choose how the report handles inactive identities. Select **No selection** to include both inactive and active identities, **True** to include only inactive identities, or **False** to not include inactive identities.

Identity Extended Attributes

You can use the identity extended attributes that have been defined for your installation as criteria for this report. Because these are custom-defined attributes, the specific criteria options you have here will be specific to your own installation of IdentityIQ. Any identity extended attributes **defined as searchable or as multi-valued** are included as possible filters for the report.

Additional Identity Details

The following criteria determines what information is included in this report. You can use any combination of options to build a report.

Option	Description
Applications	Select the applications to include in the report. If no applications are specified, all applications are included. Click the arrow to the right of the suggestion field to display a list of all applications, or enter a few letters in the field to display a list of applications that start with that letter string.
Capabilities	Include only identities assigned one or more of the selected capabilities.
Roles	Include only identities who hold the selected role(s).
Groups	Include only identities who are part of one or more of the selected group(s).
Last Refresh Date	Select a date range to filter users based on when the user was last refreshed.
Last Login Date	Select a date range to filter users based on when the user was last logged in.

User Details Report

This report shows each identity's name, first name, last name, and manager, plus a list of all roles assigned to or detected for each identity and a list of all applications on which each identity has accounts. If roles are specified as filters for the report, only users with those roles will be listed, but all roles connected to each listed identity will appear in their Roles column. Likewise, all applications on which the user has an account will appear in the Applications column, even if the report is filtered by a specific application.

This report includes information in the detailed results format that can be exported to a .csv file and used as spreadsheets.

The User Details Report consists of the following sections:

- Standard Report Properties
- Identity Attributes
- Identity Extended Attributes
- Additional Identity Properties
- Report Layout

All reports use a set of standard properties for basic information, such as naming and descriptions, and to set controls, such as scope and to required sign off.

You must enter the following before running this report:

- Name

For step by step instructions on creating or editing a report, see Working With Reports

Identity Attributes

The following criteria determines what information is included in this report. You can use any combination of options to build a report.

Option	Description
First Name	Input the first name of the identity you wish the report to include. For example, if you input "John" in the field, the report includes information on identities whose first name is John.
Last Name	Input the last name of the identity you wish the report to include. For example, if you input "Smith" in the field, the report includes information on identities whose last name is Smith.
Display Name	Input the display name of the identity you wish the report to include. For example, if you input "John_Smith" in the field, the report includes information on identities whose display name is John_Smith.
Email	Input the email address of the identity you wish the report to include. For example, if you input "John@email.com" in the field, the report includes information on identities whose email address is name is John@email.com.
Manager	The manager list to include in this report. Only users who report to the selected managers are included in the report. Click the arrow to the right of the suggestion field to a list of all managers, or enter a few letters in the field to display a list of managers that start with that letter string.

Option	Description
Inactive	Choose how the report handles inactive identities. Select **No selection** to include both inactive and active identities, **True** to include only inactive identities, or **False** to not include inactive identities.

Identity Extended Attributes

You can use the identity extended attributes that have been defined for your installation as criteria for this report. Because these are custom-defined attributes, the specific criteria options you have here will be specific to your own installation of IdentityIQ. Any identity extended attributes **defined as searchable or as multi-valued** are included as possible filters for the report.

Additional Identity Properties

The following criteria determines what information is included in this report. You can use any combination of options to build a report.

Option	Description
Applications	Select the applications to include in the report. If no applications are specified, all applications are included. Click the arrow to the right of the suggestion field to display a list of all applications, or enter a few letters in the field to display a list of applications that start with that letter string.
Capabilities	Include only identities assigned one or more of the selected capabilities.
Roles	Include only identities who hold the selected role(s).
Groups	Include only identities who are part of one or more of the selected group(s)
Last Refresh Date	Select a date range to filter users based on when the user was last refreshed. Date ranges can be open-ended in either direction (no start or no end date), as needed.
Last Login Date	Select a date range to filter users based on when the user was last logged in. Date ranges can be open-ended in either direction (no start or no end date), as needed.

Users by Application Report

This report lists the identities connected to each account on one or more applications defined in the system. For each account, it shows the associated Identity name, the account native identity (as Account Id), and the account display name (as Account Name). By default, the report includes all applications, but it can be filtered to show only accounts for specific applications.

This report includes information in the detailed results format that can be exported to a .csv file and used as spreadsheets.

The Users by Application Detail Report consists of the following sections:

- Standard Report Properties
- Report Options. These are described in the table below.

- Report Layout

All reports use a set of standard properties for basic information, such as naming and descriptions, and to set controls, such as scope and to required sign off.

You must enter the following before running this report:

- Name

For step by step instructions on creating or editing a report, see Working With Reports

Report Options

The following criteria determines what information is included in this report. You can use any combination of options to build a report.

> Selecting NO options from a list indicates that ALL options in the list are included in the report.

Option	Description
Applications	Select the applications to include in the report. If no applications are specified, all applications are included. Click the arrow to the right of the suggestion field to display a list of all applications, or enter a few letters in the field to display a list of applications that start with that letter string.

Policy Violation Report

This report details policy violations detected for identities. It shows which policies, and rules within the policies, were violated by which user, the violation owner for each, the current status of each violation, and a brief summary or description of each. (The Summary column either shows the description value for the violation, or displays the lists of mutually exclusive roles in a separation of duties policy, or displays the description on the policy constraint itself.)

The report also includes a summary section made up of a summary table and a graph. The table shows the number of violations included in the report, the number of identities involved in that violation set, and the number of open violations and mitigated violations in the set. The chart shows the numbers of violations of each policy type in graphical form.

This report includes information in the detailed results format that can be exported to a .csv file and used as spreadsheets.

The Policy Violation Report consists of the following sections:

- Standard Report Properties
- Policy Violation Properties. These are described in the table below.
- Report Layout

All reports use a set of standard properties for basic information, such as naming and descriptions, and to set controls, such as scope and to required sign off.

You must enter the following before running this report:

- Name

For step by step instructions on creating or editing a report, see Working With Reports

Policy Violation Properties

The following criteria determines what information is included in this report. You can use any combination of options to build a report.

> Selecting NO options from a list indicates that ALL options in the list are included in the report.

Option	Description
Identities	Select the identities to include in the report. If no identities are specified, all identities are included. Click the arrow to the right of the suggestion field to display a list of all identities, or enter a few letters in the field to display a list of identities that start with that letter string. Only violations associated with the selected identities are included in the report.
Policy	The policies to include in this report. Only violations of the policies selected from the list are included in the report.
Violation Activity	Show only violations of active policies, only violations of no longer active policies, or all violations (only relevant after running an identity refresh task with both the Check active policies and Keep previous violations options selected)
Violation Date	Only the violations detected on or before this date are included in the report.
Violation Status	Use to filter the report by violation status type. Choose from Open Violations, Inactive Violations, and All Violations.

Risk Reports

- Applications Risk Live Report
- Identity Risk Live Report
- Risky Accounts Report

Applications Risk Live Report

This report shows the composite risk score for each application along with the component scores that were used to calculate that composite score. Disabled application risk score components are not included on the report.

Summary reports include mainly charts, graphs and summary statistics that highlight status of different areas within IdentityIQ. These reports cannot be exported to the CSV format.

The Application Risk Live Report consists of the following sections:

- Standard Report Properties
- Report Options. These options are described in the table below.
- Report Layout

All reports use a set of standard properties for basic information, such as naming and descriptions, and to set controls, such as scope and to required sign off.

You must enter the following before running this report:

- Name

For step by step instructions on creating or editing a report, see Working With Reports

Report Options

The following criteria determines what information is included in this report. You can use any combination of options to build a report.

> Selecting NO options from a list indicates that ALL options in the list are included in the report.

Option	Description
Applications	Select the applications to include in the report. If no applications are specified, all applications are included. Click the arrow to the right of the suggestion field to display a list of all applications, or enter a few letters in the field to display a list of applications that start with that letter string.
Owners	The application owners to include in the report. Only applications associated with selected application owners are included in the report Click the arrow to the right of the suggestion field to display a list of all owners, or enter a few letters in the field to display a list of owners that start with that letter string.

Identity Risk Live Report

This report shows the total risk score, and the component risk scores used to calculate it, for each Identity. It also shows the Identity's name, first name, and manager.

The summary section of this report shows a graph of the number of identities with risk scores in various score ranges. Total and component risk scores are all graphed in separate color-coded columns, and scores are subdivided into ranges of 200 points each.

This report includes information in the detailed results format that can be exported to a .csv file and used as spreadsheets.

The Identity Risk Live Report consists of the following sections:

- Standard Report Properties
- Identity Attributes
- Identity Extended Attributes
- Additional Identity Details
- Report Layout

All reports use a set of standard properties for basic information, such as naming and descriptions, and to set controls, such as scope and to required sign off.

You must enter the following before running this report:

- Name

For step by step instructions on creating or editing a report, see Working With Reports

Identity Attributes

The following criteria determines what information is included in this report. You can use any combination of options to build a report.

> Selecting NO options from a list indicates that ALL options in the list are included in the report.

> Use the Shift and Crtl keys to select multiple items from lists.

Option	Description
First Name	Input the first name of the identity you wish the report to include. For example, if you input “John” in the field, the report includes information on identities whose first name is John.
Last Name	Input the last name of the identity you wish the report to include. For example, if you input “Smith” in the field, the report includes information on identities whose last name is Smith.
Display Name	Input the display name of the identity you wish the report to include. For example, if you input “John_Smith” in the field, the report includes information on identities whose display name is John_Smith.
Email	Input the email address of the identity you wish the report to include. For example, if you input “John@email.com” in the field, the report includes information on identities whose email address is name is John@email.com.
Managers	The manager list to include in this report. Only users who report to the selected managers are included in the report. Click the arrow to the right of the suggestion field to a list of all managers, or enter a few letters in the field to display a list of managers that start with that letter string.
Inactive	Choose how the report handles inactive users. Select **No selection** to include both inactive and active users, **True** to include only inactive users, or **False** to not include inactive users.

Identity Extended Attributes

You can use the identity extended attributes that have been defined for your installation as criteria for this report. Because these are custom-defined attributes, the specific criteria options you have here will be specific to your own installation of IdentityIQ. Any identity extended attributes **defined as searchable or as multi-valued** are included as possible filters for the report.

Additional Identity Details

The following criteria determines what information is included in this report. You can use any combination of options to build a report.

> Selecting NO options from a list indicates that ALL options in the list are included in the report.

> Use the Shift and Crtl keys to select multiple items from lists.

Option	Description
Applications	Select the applications to include in the report. If no applications are specified, all applications are included. Click the arrow to the right of the suggestion field to display a list of all applications, or enter a few letters in the field to display a list of applications that start with that letter string.
Capabilities	Select the capabilities to include in the report.
Roles	The roles to include in the report. Click the arrow to the right of the field and select a role to create the inclusion list for this report.
Groups	The groups or populations to include in the report. Click the arrow to the right of the field and select a group to create the inclusion list for this report.
Last Refresh Date	Select a date range to filter users based on when the user was last refreshed.
Last login Date	Specify a login date range manually or click the calendar icon and select one using the calendar options.

Risky Accounts Report

This report lists identities with accounts which represent risk on applications (that is, cause a higher application risk score for the application), along with the issues that cause the accounts to be identified as risky.

Summary reports include mainly charts, graphs and summary statistics that highlight status of different areas within IdentityIQ. These reports cannot be exported to the CSV format.

The Risky Accounts Report consists of the following sections:

- Standard Report Properties
- Report Options. These are described in the table below.
- Report Layout

All reports use a set of standard properties for basic information, such as naming and descriptions, and to set controls, such as scope and to required sign off.

You must enter the following before running this report:

- Name

For step by step instructions on creating or editing a report, see Working With Reports

Report Options

The following criteria determines what information is included in this report. You can use any combination of options to build a report.

> Selecting NO options from a list indicates that ALL options in the list are included in the report.

Option	Description
Correlated Applications	Select the applications to include in the report. If no applications are specified, all applications are included. Click the arrow to the right of the suggestion field to display a list of all applications, or enter a few letters in the field to display a list of applications that start with that letter string. Correlated Applications are applications that are to be compared with the authoritative application. Any identity that has an account on the correlated application but not on the authoritative application is considered uncorrelated.

Role Management Reports

Role analytics are an important part of the overall role life-cycle management. Role analytics provide role managers the ability to be proactive in their approach to monitoring and improving the role model within your organization. Role modeling is an iterative and constant process. As your business needs change, security features improve, and new applications and user are added to your enterprise, your role model will have to change accommodate them. Use role analytics to keep up with those changing needs and adjust your model as needed.

- Identity Roles Report
- Role Archive Report
- Role Change History Report
- Role Details Report
- Role Members Report
- Role Profiles Composition Report
- Roles by Application Report

Identity Roles Report

This report shows all of the roles connected to a set of identities. It indicates whether each role was assigned to or detected on the identity, and it shows the last time that role was certified for the identity. Note that detected roles which were certified as a part of assigned roles (i.e. they were required/permitted by assigned roles that were certified) will not have a certification date shown next to them, but detected roles that are not granted by assigned roles and are therefore certified independently will show a certification date.

This report includes information in the detailed results format that can be exported to a .csv file and used as spreadsheets.

The Identity Roles Report consists of the following sections:

- Standard Report Properties
- Identity Attributes
- Identity Extended Attributes
- Additional Identity Properties
- Report Layout

All reports use a set of standard properties for basic information, such as naming and descriptions, and to set controls, such as scope and to required sign off.

You must enter the following before running this report:

- Name

For step by step instructions on creating or editing a report, see Working With Reports

Identity Attributes

The following criteria determines what information is included in this report. You can use any combination of options to build a report.

> Selecting NO options from a list indicates that ALL options in the list are included in the report.

> Use the Shift and Crtl keys to select multiple items from lists.

Option	Description
First Name	Input the first name of the identity you wish the report to include. For example, if you input “John” in the field, the report includes information on identities whose first name is John.
Last Name	Input the last name of the identity you wish the report to include. For example, if you input “Smith” in the field, the report includes information on identities whose last name is Smith.
Display Name	Input the display name of the identity you wish the report to include. For example, if you input “John_Smith” in the field, the report includes information on identities whose display name is John_Smith.
Email	Input the email address of the identity you wish the report to include. For example, if you input “John@email.com” in the field, the report includes information on identities whose email address is name is John@email.com.
Manager	The manager list to include in this report. Only users who report to the selected managers are included in the report. Click the arrow to the right of the suggestion field to a list of all managers, or enter a few letters in the field to display a list of managers that start with that letter string.
Inactive	Choose how the report handles inactive users. Select **No selection** to include both inactive and active users, **True** to include only inactive users, or **False** to not include inactive users.

Identity Extended Attributes

You can use the identity extended attributes that have been defined for your installation as criteria for this report. Because these are custom-defined attributes, the specific criteria options you have here will be specific to your own installation of IdentityIQ. Any identity extended attributes **defined as searchable or as multi-valued** are included as possible filters for the report.

Additional Identity Properties

The following criteria determines what information is included in this report. You can use any combination of options to build a report.

> Selecting NO options from a list indicates that ALL options in the list are included in the report.

> Use the Shift and Crtl keys to select multiple items from lists.

Option	Description
Applications	Select the applications to include in the report. If no applications are specified, all applications are included. Click the arrow to the right of the suggestion field to display a list of all applications, or enter a few letters in the field to display a list of applications that start with that letter string.
Capabilities	Select the capabilities to include in the report.
Roles	The roles to include in the report. Click the arrow to the right of the field and select a role to create the inclusion list for this report.
Groups	The groups or populations to include in the report. Click the arrow to the right of the field and select a group to create the inclusion list for this report.
Last Refresh Date	Select a date range to filter users based on when the user was last refreshed.
Last Login Date	Select a date range to filter users based on when the user was last logged in.

Role Archive Report

This report shows a detailed view of each role defined in the system (subject to filter criteria). Each page lists a single role and shows details such as its owner, activity monitoring status, activation status, type, inheritance, and as applicable to the role type, its permitted/required roles, detection profiles, among others.

This report is an archive-type report. Archive reports include end-of-period and task information that is formatted for easy dissemination of key audit information. Due to the large amount of data that is generated, the best option is to export the report results to a .pdf file.

The Role Archive Report consists of the following sections:

- Standard Report Properties
- Role Report Options. These are described in the table below.
- Report Layout

All reports use a set of standard properties for basic information, such as naming and descriptions, and to set controls, such as scope and to required sign off.

You must enter the following before running this report:

- Name

For step by step instructions on creating or editing a report, see Working With Reports

Role Report Options

The following criteria determines what information is included in this report. You can use any combination of options to build a report.

> Selecting NO options from a list indicates that ALL options in the list are included in the report.

Option	Description
Applications	Select the applications to include in the report. If no applications are specified, all applications are included. Click the arrow to the right of the suggestion field to display a list of all applications, or enter a few letters in the field to display a list of applications that start with that letter string. Only roles associated with the selected applications are included in this report.
Type	Select types of roles to include in the report.
Owners	The list of role owners to include in this report. If no role owners are specified, the roles for all owners are included. Click the arrow to the right of the suggestion field to display a list of all role owners, or enter a few letters in the field to display a list of role owners that start with that letter string.
Status	Include only active roles or only inactive roles in the report.

Role Change History Report

This report shows a summary of the roles which have been altered during the specified time period, the date of the alteration, and the name of the change approver. This report is based on the existence of role archives, so it can only be run for installations that have enabled role archiving (set the “doArchive” variable to “true” in the selected role management workflow). The person whose name is associated with the creation of the RoleArchive object is listed as the approver on the report; this may be the person who made the change or may be a separate approver, depending on the approval mode configured in the system.

This report includes information in the detailed results format that can be exported to a .csv file and used as spreadsheets.

The Role Change History Report consists of the following sections:

- Standard Report Properties
- Role Properties. These are described in the table below.
- Report Layout

All reports use a set of standard properties for basic information, such as naming and descriptions, and to set controls, such as scope and to required sign off.

You must enter the following before running this report:

- Name

For step by step instructions on creating or editing a report, see Working With Reports

Role Properties

The following criteria determines what information is included in this report. You can use any combination of options to build a report.

> Selecting NO options from a list indicates that ALL options in the list are included in the report.

Option	Description
Change Start and End Date (s)	Filter request based on request date: **Start Date** — all changes made on or after the selected date. **End Date** — all changes made on or before the selected date.
Role Status	Include only active roles or only inactive roles in the report.
Type	Select types of roles to include in the report.
Applications	Select the applications to include in the report. If no applications are specified, all applications are included. Click the arrow to the right of the suggestion field to display a list of all applications, or enter a few letters in the field to display a list of applications that start with that letter string. Only roles associated with the selected applications are included in this report.
Owners	The list of role owners to include in this report. If no role owners are specified, the roles for all owners are included. Click the arrow to the right of the suggestion field to display a list of all role owners, or enter a few letters in the field to display a list of role owners that start with that letter string.

Role Details Report

The Role Details Report includes information on the role name, owner name, role type, and associated applications configured in IdentityIQ, for each role that matches the specified criteria.

This report includes information in the detailed results format that can be exported to a .csv file and used as spreadsheets.

The Role Details Report consists of the following sections:

- Standard Report Properties
- Report Criteria. These options are described in the table below.
- Report Layout

All reports use a set of standard properties for basic information, such as naming and descriptions, and to set controls, such as scope and to required sign off.

You must enter the following before running this report:

- Name

For step by step instructions on creating or editing a report, see Working With Reports

Report Criteria

The following criteria determines what information is included in this report. You can use any combination of options to build a report.

> Selecting NO options from a list indicates that ALL options in the list are included in the report.

Option	Description
Role Status	Include only active roles or only inactive roles in the report.
Applications	Select the applications to include in the report. If no applications are specified, all applications are included. Click the arrow to the right of the suggestion field to display a list of all applications, or enter a few letters in the field to display a list of applications that start with that letter string. Only roles associated with the selected applications are included in this report.
Owners	The list of role owners to include in this report. If no role owners are specified, the roles for all owners are included. Click the arrow to the right of the suggestion field to display a list of all role owners, or enter a few letters in the field to display a list of role owners that start with that letter string.
Role Type	Select types of roles to include in the report.
Show Applications for Indirect Roles	If your role model uses indirect roles (for example, if you map business roles to IT roles), use this option to include application information for indirect roles. Note that selecting this option may impact report performance. You can also use the Roles by Application Report to report on indirect roles, with more streamlined performance.
Show Inherited Applications	If a role (whether direct or indirect) inherits any entitlements, select this option to display the names of the applications for the inherited entitlements. Note that selecting this option may impact report performance. You can also use the Roles by Application Report to report on inherited, with more streamlined performance.

Role Members Report

This report shows the names of all Identities who are associated to each role that meets the specified report filters. Identities are considered “members” of a role if the role is in either their assigned or detected role set.

This report includes information in the detailed results format that can be exported to a .csv file and used as spread-sheets.

The Role Members Report consists of these sections:

- Standard Report Properties
- Role Members Options. These options are described in the table below.
- Report Layout

All reports use a set of standard properties for basic information, such as naming and descriptions, and to set controls, such as scope and to require sign off.

You must enter the following before running this report:

- Name

For step by step instructions on creating or editing a report, see Working With Reports

Role Members Options

The following criteria determines what information is included in this report. You can use any combination of options to build a report.

> Selecting NO options from a list indicates that ALL options in the list are included in the report.

Option	Description
Role Status	Include only active roles or only inactive roles in the report.
Applications	Select the applications to include in the report. If no applications are specified, all applications are included. Click the arrow to the right of the suggestion field to display a list of all applications, or enter a few letters in the field to display a list of applications that start with that letter string.
Role Owners	To filter roles by role owner, choose the owner(s) here. If no role owners are specified, the roles for all owners are included. Click the arrow to the right of the suggestion field to display a list of all role owners, or enter a few letters in the field to display a list of role owners that start with that letter string.
Type	To filter roles by type, select types here. If no types are selected. all types of roles are included.
Empty Roles	Filter for role membership: select All Roles, Only Empty Roles (to include only roles with no members) or Only Populated Roles (to

Option	Description
	include only roles with members assigned).
Role Name	Choose roles to include in the report, by name. Click the arrow to display a list of all roles, or enter a few letters in the field to display a list of roles that start with that letter string. Leave this field blank to include all roles.

For the next four fields, the values you can choose are determined by the application(s) you have selected.

If no application is selected, the drop-down will show all valid options for all applications in the system.

If the application(s) you have selected do not have any valid options for the field, the drop-down is replaced by a text box. You can type in any values and click the plus icon to add them as criteria, but any invalid options entered in this way are "sanitized" when the report is run, and will not produce results or appear in the report's list of parameters.

Entitlement Attribute	Filter for roles that include the selected entitlement attribute(s).
Entitlement Value	Filter for roles that include the selected entitlement value(s).
Permission Target	Filter for roles that include the selected permission target(s).
Permission Right	Filter for roles that include the selected permission right(s).
Profile Relationship to Role	Filter roles by the role's profile relationship (direct or indirect). A profile is a set of entitlements on a specific application. Options are: • Any direct or indirect relationships • Any direct relationships • Any indirect relationships This filter is typically used in conjunction with an application, and the entitlement or permission filters. For example, to filter for a role that provides direct access to the PayrollControls permission target on the Oasis_DB application, you would select the **Oasis_DB** application, select **PayrollControls** in the **Permission Target** field, and choose **Any direct relationships** here. Note that some roles can grant both direct and indirect access to entitlements and permissions, so a role can potentially be returned by both the direct relationship and indirect relationship options.

Role Profiles Composition Report

This report shows the profiles used for role detection. If a description was provided for the profile, it is included in the report along with the filter used for role detection and the application against which the filter is applied. If a role includes more than one profile filter (for example, to specify criteria on multiple applications), each one is included as a separate line item on the report. Roles without profiles are noted with “Contains No Profiles” in the description column; under the default IdentityIQ role configuration, any non-IT role will be marked as containing no profiles since profiles are specific to IT roles only.

This report returns information in the detailed results format that can be exported to a .csv file and used as spreadsheets.

The Role Profiles Composition Report consists of the following sections:

- Standard Report Properties
- Role Properties. These are described in the table below.
- Report Layout

All reports use a set of standard properties for basic information, such as naming and descriptions, and to set controls, such as scope and to required sign off.

You must enter the following before running this report:

- Name

For step by step instructions on creating or editing a report, see Working With Reports

Role Properties

The following criteria determines what information is included in this report. You can use any combination of options to build a report.

> Selecting NO options from a list indicates that ALL options in the list are included in the report.

Option	Description
Role Status	Include only active roles or only inactive roles in the report.
Roles Without Profiles	Include only roles that contain no profiles or only roles that contain at least one profile.
Applications	Select the applications to include in the report. If no applications are specified, all applications are included. Click the arrow to the right of the suggestion field to display a list of all applications, or enter a few letters in the field to display a list of applications that start with that letter string. Only roles associated with the selected applications are included in this report.
Owners	The list of role owners to include in this report. If no role owners are specified, the roles for all owners are included. Click the arrow to the right of the suggestion field to display a list of all role owners, or enter a few letters in the field to display a list of role owners that start with

Option	Description
	that letter string.
Type	Select types of roles to include in the report.

Roles by Application Report

The Roles by Application Report shows role relationships for all applications. You can run this report on all applications, or on selected applications.

The Roles by Application Report includes the following sections:

- Standard Report Properties
- Role Properties. These are described in the table below.
- Report Layout

All reports use a set of standard properties for basic information, such as naming and descriptions, and to set controls, such as scope and to required sign off.

You must enter the following before running this report:

- Name

For step by step instructions on creating or editing a report, see Working With Reports

Role Properties

The following criteria determines what information is included in this report.

Option	Description
Applications	Select the application(s) to include in the report. If no applications are selected, all applications are included. To select the applications to include, click the arrow in the suggestion field to see a list of all applications, or enter a few letters in the field to display a list of applications that start with that letter string. Only roles associated with the selected applications are included in this report.
Show role relations for all applications	This option is available only if you have not selected specific applications to report on, in the **Applications** field. Use this option to list all direct, required, and permitted applications for all roles.
Include roles with inherited entitlements	Use this option to include roles that inherit application entitlements.

Roles by Entitlement Report

The Roles by Entitlement Report shows how particular entitlements and permissions fit into your organization's role model. This report lets you enter specific entitlements or permissions for selected application(s) and see which roles provide direct or indirect access to them. You must select at least one application as part of your reporting critiera (in other words, you can not leave the Application field blank to report on all applications at once).

The Roles by Entitlement Report includes the following sections:

- Standard Report Properties
- Role Properties. These are described in the table below.
- Report Layout

All reports use a set of standard properties for basic information, such as naming and descriptions, and to set controls, such as scope and to required sign off.

You must enter the following before running this report:

- Name
- Application
- Filter Type

For step by step instructions on creating or editing a report, see Working With Reports

Role Properties

The following criteria determines what information is included in this report.

Option	Description
Applications	Select the application(s) to include in the report. **You must select at least one application.** Click the arrow in the suggestion field to see a list of all applications, or enter a few letters in the field to display a list of applications that start with that letter string. Only roles associated with the selected applications are included in this report.
Filter Type	Choose whether to report on role relationships based on **entitlements** or on **permissions**. A selection in this field is required. The selection you make here determines which of the following fields appear: **Entitlement** fields or **Permission** fields.
Entitlement Attribute	Filter for roles that include the selected entitlement attribute(s).
Entitlement Value	Filter for roles that include the selected entitlement value(s).
Permission Target	Filter for roles that include the selected permission target(s).
Permission Right	Filter for roles that include the selected permission right(s).
Profile Relationship to Role	Filter roles by the role's profile relationship (direct or indirect). A profile is a set of entitlements on a specific application. Options are: • Any direct or indirect relationships

Option	Description
	• Any direct relationships • Any indirect relationships For example, to filter for a role that provides *direct* access to both the **AcctsPayable** and **AcctsReceiveable** groups in the Accounting application, you would select the **Accounting** application, choose **Entitlements** as the Filter Type, and enter **AcctsPayable** and **AcctsReceiveable** in the **Entitlement Value** field. Then choose **Any direct relationships** here. Note that some roles can grant both direct and indirect access to entitlements and permissions, so a role can potentially be returned by both the direct relationship and indirect relationship options.

Developing Custom Reports

IdentityIQ includes a reporting architecture that greatly simplifies the process of developing custom reports by allowing the developer to specify the report requirements in a TaskDefinition XML document. The executor uses IdentityIQ's Forms API to generate the UI form for specifying parameters, and creates the report output based on column configurations specified in the TaskDefinition. The XML specifies the report's Standard Properties values, the report-specific parameters, the columns that are available for the report, how the data is retrieved for inclusion on the report, and how the report results are laid out in both the detail and summary sections.

The standard report templates provide some good examples of how to define reports through XML. Excerpts from these standard templates are used in this section to illustrate how to configure custom reports. Many of the excerpts come from the Uncorrelated Accounts Report, a simple example that can be used to explore the basics of defining a custom report.

It can be helpful to examine the full XML for these reports to see the tags' usage in context as they are referenced and excerpted in this section. The reports can be viewed through the Debug pages as described in XML Representation of Reports and Instances, or the entire set of TaskDefinition objects can be exported to a file through the iiq console and explored in a text editor. The console export command to write the system's TaskDefinition objects to a file is "`export taskDefs.xml TaskDefinition`" (where "taskDefs.xml" is the name of the file to which the objects are exported). Note that the file contains all tasks including reports because no filter available on the export command to select only a subset of objects of a given type.

See:

Reports in the IdentityIQ Object Model

Report Definition

Report Forms

Reports DataSource Example

Reports in the IdentityIQ Object Model

In IdentityIQ, a report is executed as a specialized **task**. The root element of a report in the object model is a `<TaskDefinition>` element. Report results are stored in the object model as `<TaskResult>` objects.

```
<TaskDefinition executor="sailpoint.reporting.LiveReportExecutor" name="Uncorrelated
Accounts Report" progressMode="Percentage" resultAction="Rename" subType="Identity and
User Reports" template="true" type="LiveReport">
```

In the example above, the **type attribute** for the TaskDefinition indicates that this is a report definition, and the **executor** specifies which class processes this task definition to run the report. The attributes of the TaskDefinition object and their purposes are described below.

Attribute	Usage
executor	The class used to run the report. The "sailpoint.reporting.LiveReportExecutor",

Attribute	Usage
	is always specified as the executor for any report of type “LiveReport,” including custom reports.
name	Name of the report template; shown on the **Reports** list as the report's **Name** When templates are edited, they must be saved as customized report instances, and the name value across all report templates and report instances must be unique. Therefore, the name attribute for a template is not displayed as the Name field's value on the Edit Report window's Standard Properties page since instances cannot be saved with this same name. The value entered in the Standard Properties page's Name field becomes the name value of the TaskDefinition XML for that instance.
progressMode	Specifies how the executor updates progress while the report is being executed; most reports use Percentage. Possible values are: **None** — executor doesn't update progress (same as null, or not specifying) **String** — executor periodically updates progressString property of the result during execution **Percentage** — executor periodically updates the progress and per-centageComplete properties of the result during execution
resultAction	Specifies the **PreviousResultAction** (shown on the Standard Properties page) which determines how to manage the results from previous runs of this report when it is executed again. Possible values are: **Rename** — rename old report results by appending a numeric value (for example, Uncorrelated Accounts Report - 2) **RenameNew** — rename new report results by appending a numeric value **Cancel** — do not run the report when old report results still exist for the report (displays an error message indicating that a result from a previous execution of the report still exists) **Delete** — delete old report results when the report is executed again
subType	The report category to which this report belongs (sub-categories within the **Reports** and **My Reports** tabs); can be one of the out-of-the-box subTypes or a custom subType
template	Boolean indicating whether this is a report template (appears on the **Reports** tab) or a customized report instance (appears on **My Reports** tab); new cus-tom reports should be set up as template=”true”
type	All reports, including new custom reports, are of type “LiveReport”

See, Elements within TaskDefinition

Elements within TaskDefinition

The TaskDefinition contains several nested elements that are used to define important information for the report. The TaskDefinition always contains an Attributes map and a Signature, and usually contains a Description element and a list of RequiredRights.

Attributes Map

The **Attributes** map must at minimum include the report definition.

```
 <Attributes>
      <Map>
        <entry key="report">
          <value>
            <LiveReport title="Uncorrelated Accounts Report">
                …
            </LiveReport>
          </value>
        </entry>
      </Map>
    </Attributes>
```

Other optional attributes in the attribute map include emailIdentities, reportSortBy, reportGroupBy, disableSummary, and disableDetail, as described in the Standard Forms for Report Specification section.

Signature

The Signature contains a map of Input attributes that name all of the parameters that can be specified for the report.

```
<Signature>
    <Inputs>
      <Argument multi="true" name="correlatedApps" type="Application">
        <Description>rept_input_uncorrelated_ident_report_correlated_apps
        </Description>
        <Prompt>report_input_correlated_apps</Prompt>
      </Argument>
      <Argument name="resultScope" type="Scope">
        <Description>rept_input_result_scope</Description>
      </Argument>
      <Argument multi="true" name="emailIdentities" type="Identity">
        <Description>rept_input_email_recips</Description>
      </Argument>
    </Inputs>
 </Signature>
```

When a customized report instance with pre-populated parameters is saved, those parameters are saved as a part of the instance's TaskDefinition in its Attributes map. In this example, a list of Applications and a list of Email Recipients have been saved for this report instance.

```
<TaskDefinition created="1344453735712" id="4028460238edaba4013907aff5200ec9" mod-
ified="1344867911170" name="Uncorrelated Accounts" resultAction="Rename" sub-
Type="Identity and User Reports" type="LiveReport">
 <Attributes>
    <Map>
       <entry key="correlatedApps">
        <value>
          <List>
```

```
            <String>4028460238edaba401372767b6eb0d70</String>
            <String>4028460238edaba40138edcfcd1102d2</String>
          </List>
        </value>
      </entry>
      <entry key="disableDetail" value="false"/>
      <entry key="disableSummary" value="false"/>
      <entry key="emailIdentities">
        <value>
          <List>
            <String>4028460238edaba40138edb3571e000d</String>
          </List>
        </value>
      </entry>
      <entry key="reportColumnOrder" value="username, firstName, lastName"/>
    </Map>
  </Attributes>
```

They are passed from the customized report instance to the associated report template at run-time through the taskDefinition input arguments specified in the `<Signature>` for the report.

Every report template's Signature should include input arguments for resultScope and emailIdentities, since these automatically appear on the Standard Properties window and are available for a user to specify on all reports. All other input arguments are report-specific and the remainder of the arguments in a custom report is specific to that report. The list of arguments should match the set of fields available for parameter specification on the report's Form. Report-specific arguments should include a name and type as attributes on the `<Argument>` element. If the argument is multi-valued, it should also include the attribute “multi=”true”.”

Application arguments can include a Description and Prompt element. When a custom form (in a `<ReportForm>` element) has been specified, these are ignored and can be omitted. However, if no custom form is specified, these report-specific input arguments are automatically rendered on a form page (titled Report Options) using the Prompt value as the field label and the Description value as the tool tip for the field. Both of these values can be specified as strings or as localizable message keys.

```
<Argument multi="true" name="correlatedApps" type="Application">
 <Description>rept_input_uncorrelated_ident_report_correlated_apps
 </Description>
 <Prompt>report_input_correlated_apps</Prompt>
```

The Account Group Members report is an example of a report that relies on this automatic form rendering for its report-specific filter options.

Description

The Description element is displayed as the Description for the report on both the Reports and My Reports lists and on the Edit Report window.

```
<Description>A detailed view of the uncorrelated user accounts in the sys-
tem.</Description>
```

Required Rights

The RequiredRights element specifies what system right(s) a user must have to be able to see and execute the report. The required rights are specified as references to one or more SPRight objects.

```
<RequiredRights>
   <Reference class="sailpoint.object.SPRight" id="4028460238ed9b8e0138ed9bc59d0054" name-
e="FullAccessUncorrelatedIdentitiesReport"/>
</RequiredRights>
```

Report Definition

The report, including its custom UI form or forms, its query specification, and its results contents and layout, is specified as a part of the TaskDefinition's attributes map with the attribute key “report”. The value for this attribute is a <LiveReport> element.

```
<Attributes>
    <Map>
      <entry key="report">
        <value>
          <LiveReport title="Uncorrelated Accounts Report">
```

Elements within <LiveReport> determine the report filters that can be specified by a report user, the query used to retrieve the data for the report, the layout of the report detail grid, and the contents and layout of the report's summary table and chart. The nested elements within <LiveReport> are:

Element	Description
ReportForm	Determines how the report-specific parameters sections are presented to the user in the Edit Report window (see ReportForm: Collecting Report-Specific Parameters)
DataSource	Specifies how the data for the report details is retrieved from the database (see DataSource: Retrieving Report Data)
Columns	Lists columns available for inclusion in the report detail grid; also used in conjunction with DataSource to determine which data elements are retrieved in the query (see Columns/ReportColumnConfig: Report Grid Presentation)
ReportSummary	Describes the Summary section of the report - information included, query to retrieve it, layout and labels for presentation of it (see ReportSummary: Summary Table)
Chart	Defines the graph or chart displayed in the Summary section for the report (see Chart: Report Graph)

For more information, see:

ReportForm: Collecting Report-Specific Parameters

DataSource: Retrieving Report Data

Columns/ReportColumnConfig: Report Grid Presentation

ReportForm: Collecting Report-Specific Parameters

Most reports allow you to set filters that constrain the contents of the generated report. In custom reports, report-specific parameters are collected from the report user through a custom form, that is referenced through a ReportForm element in the report definition. The form must be specified as a separate XML document and imported into IdentityIQ. The Form object is described in Report Forms.

The ReportForm element references the form like this:

```
<ReportForm>
<Reference class="sailpoint.object.Form" id="4028460238edaba40138edb36b330010" name-
e="Uncorrelated Account Report Custom Fields"/>
</ReportForm>
```

Standard Forms for Report Specification

The referenced ReportForm is presented to the user in the Edit Report window between the two standard form pages that are part of every report's specification: Standard Properties and Report Layout. Those two standard pages are rendered based on a Form object called Report Skeleton using values specified in the report's TaskDefinition XML. These tables indicate which TaskDefinition elements and attributes determine the values for fields on the Standard Properties and Report Layout pages.

Standard Properties Field	TaskDefinition Source
Name	If editing a customized report instance, <TaskDefinition> name attribute `<TaskDefinition name="Uncorrelated Accounts - Financials" … >` If creating a new report instance based on a template, none (not populated)
Previous Result Action	`<TaskDefinition> resultAction attribute<TaskDefinition name="Uncorrelated Accounts Report" resultAction="Rename" … >`
Description	<Description> element

Standard Properties Field	TaskDefinition Source
Scope*	resultScope entry in Attributes map (value contains ID of selected scope) `<entry key="resultScope" value-e="2c9082ee38e813a20138e934eb210146"/>`
Email Recipients*	emailIdentities entry in Attributes map (List contains Identity ID values) `<entry key=”emailIdentities”> <value> <List> <String>4028460238edaba40138edb35653000b</String> </List> </value> </entry>` Usually specified in instance XML instead of template XML
Allow Concurrency	`<TaskDefinition> concurrent attribute (concurrent=”true”)<TaskDefinition concurrent="true" name-e="Uncorrelated Accounts Report" … >`
Require Signoff*	<SignoffConfig> element `<SignoffConfig> <WorkItemConfig created="1344962495866" escal-ationStyle="none" id="4028460238edaba401392603057a1464"> <NotificationEmailTemplateRef><Reference class-s="sailpoint.object.EmailTemplate" id="4028460238ed9b8e0138ed9bd8690106" name="Default Report Template"/> </NotificationEmailTemplateRef> <Owners><Reference class="sailpoint.object.Identity" id="4028460238edaba40138edb36b33016d" name-e="Aaron.Nichols"/> </Owners> </WorkItemConfig> </SignoffConfig>`

Report Layout Field	TaskDefinition Source
Sort By*	reportSortBy entry in Attributes map `<entry key="reportSortBy" value-e="accountGroupDisplayName"/>`

Report Layout Field	TaskDefinition Source

Sort Ascending*	reportSortAsc entry in attributes map
	
	`<entry key="reportSortAsc">`
	`<value>`
	`<Boolean>true</Boolean>`
	`</value>`
	`</entry>`

Group By*	reportGroupBy entry in Attributes map `<entry key="reportGroupBy" value="application"/>`
Columns	<ReportColumnConfig> header attributes; hidden="true" attribute places column in left pane - available but not included on report detail by default `<ReportColumnConfig field="accountGroupName" header="rept_app_account_grp_memb_col_name" property="value" sortable="true" />`
Disable Report Summary Display*	disableSummary entry in Attributes map `<entry key="disableSummary" value="true"/>`
Disable Report Detail Display*	disableDetail entry in Attributes map `<entry key="disableDetail" value="true"/>`

* These fields are typically specified through the UI for customized instances of reports and saved into the My Reports instances' attributes map, rather than being specified in the report template XML. However, they can be specified in the template XML if they apply to the report's default configuration.

Although most reports do include a custom form, it is not required. When one is not specified, the Edit Report window still displays the Standard Properties and Report Layout pages; the Identity Status Summary report shows an example of this.

DataSource: Retrieving Report Data

The data shown in the detail section of the report is retrieved through a query that is built based on a combination of the <DataSource> specification and the <Columns> element. In general, a query is specified in three parts: Select, From, and Where. The Select portion (the columns list) is specified through the <Columns> element in the report definition - specifically, the <ReportColumnConfig>s listed within <Columns> element. The From and Where clauses are specified through the <DataSource> element.

There are three available datasource types: Filter, Java, and HQL. The simplest of these three is the Filter datasource, though various options available with this datasource type make it quite powerful and flexible. The other two are available for more complex report data retrieval needs, and Java is likely to be used as the datasource more often in HQL in those cases. Each of these three datasource types is discussed next.

Filter DataSource

A filter datasource executes a projection query to retrieve the data required by the ReportColumnConfigs specified for the report. It employs the SailPoint Filter object to specify the query. The object whose data is being queried is specified as the objectType for the DataSource, and the DataSource type is specified as “Filter”.

```
<DataSource objectType="sailpoint.object.Link" type="Filter">
```

> If the objectType is one of the top-level classes in the IdentityIQ object model (for example, the set of objects that can be exported from the iiq console or retrieved directly in from the debug pages), the fully-qualified class name is not required for this attribute. For example, Identity can be specified here as objectType=”Identity”. However, the fully-qualified name (for example, sailpoint.object.Identity) is always acceptable, even for the top-level classes, so when in doubt, specify the fully-qualified name.

This is an example of a filter <DataSource> and its <Columns> specification:

```
<LiveReport title="Uncorrelated Accounts Report">
 <DataSource objectType="sailpoint.object.Link" type="Filter">
   <QueryParameters>
<Parameter argument="correlatedApps" property="application.id"/>
       <Parameter defaultValue="false" property="identity.correlated" valueClass-
s="Boolean"/>
       <Parameter defaultValue="false" property="application.authoritative" valueClass-
s="Boolean"/>
       <Parameter defaultValue="false" property="application.logical" valueClass-
s="Boolean"/>
   </QueryParameters>
 </DataSource>
 <Columns>
<ReportColumnConfig field="username" header="rept_uncorrelated_ids_grid_username" prop-
erty="nativeIdentity" sortable="true" />
<ReportColumnConfig field="firstName" header="rept_uncorrelated_ids_grid_firstName" prop-
erty="identity.firstname" sortable="true" />
<ReportColumnConfig field="lastName" header="rept_uncorrelated_ids_grid_lastName" prop-
erty="identity.lastname" sortable="true" />
<ReportColumnConfig field="applicationName" header="rept_uncorrelated_ids_grid_appName"
property="application.name" sortable="true" />
 </Columns>
```

The search criteria, making up the “where” clause for the search, are specified through one or more of several query-related elements: Query, QueryParameters, and QueryScript. Joins, sorts and groupBy columns can also be specified as needed for the query.

QueryParameters

The <QueryParameters> element is used most often. QueryParameters is a map of argument values used to create the queryOptions object that controls the search. They can be specified based on report arguments, hard-coded values, or calculated values. QueryParameters contains a list of <Parameter> elements, each of which defines one of the criteria. These <Parameter>s are "anded" together to make the where clause.

```
<QueryParameters>
```

```
    <Parameter argument="correlatedApps" property="application.id"/>
    <Parameter defaultValue="false" property="identity.correlated" valueClass="Boolean"/>
    …
</QueryParameters>
```

There are several different options for specifying parameters in a set of QueryParameters. These options are described below, illustrated with example Parameters. Most of these examples (except where noted) were taken from the Entitlement Owner Access Review Live Report which queries against the **sailpoint.object.CertificationItem** object, so all of these parameters relate to that object.

- **Referencing a report argument**: generally processed as “property = argument”; this parameter looks for certificationItems with a parent.certification.certificationGroups.id value in the report argument “certificationGroups”

  ```
  <Parameter argument="certificationGroups" property="parent.certification.certificationGroups.id"/>
  ```

  > When arguments are multi-valued, parameters based on them are automatically evaluated with “in” rather than “equals”.

- **Specifying a default value**: generally processed as “property = argument or defaultValue (if argument is null)”; this parameter looks for CertificationItems with a parent.certification.type equal to the report argument “type”; if none is provided, it defaults to the type “DataOwner”

  ```
  <Parameter argument="type" defaultValue="DataOwner" property="parent.certification.type" valueClass=
  s="sailpoint.object.Certification$Type"/>
  ```

  > This example also illustrates usage of the valueClass attribute; this attribute is not necessary for string or object comparisons but is for other types, such as enumerations (such as Type in this example), Booleans, Dates, Lists, etc.

- **Specifying a hard-coded value**: an attribute can also be hard coded to be evaluated against the defaultValue by not including an argument, as shown in this parameter from the Uncorrelated Accounts Report. This is processed as “property = defaultValue”, in this case cast as valueClass (not required for strings).

  ```
  <Parameter defaultValue=”false” property=”identity.correlated” valueClass=
  s=”boolean”/>
  ```

- **Specifying different operations**: this example illustrates how to create evaluation conditions other than equals (or in) relationships; operation can be specified as GT, GE, LT, or LE (greater than, greater than or equal to, less than, less than or equal to)

  ```
  <Parameter argument="createStartDate" operation="GT" property="parent.certification.created"/>
  ```

- **Using a ValueScript**: processed as "property = return value from ValueScript"; this parameter performs processing based on the argument to return a different value that should be used in the criterion; this example uses a ValueScript to get the application name that corresponds to the applicationID in the "application" report argument; in a ValueScript, the argument is accessed through the variable name "value".

```
<Parameter argument="applications" property="parent.application">
   <ValueScript>
      <Source>
         import sailpoint.object.*;
         import sailpoint.api.ObjectUtil;
         if (value != null){
            return ObjectUtil.convertIdsToNames(context, Application.class, value);
         }
         return null;
      </Source>
   </ValueScript>
</Parameter>
```

Since object references are stored in the customized report instance XML (and passed to report input arguments) as ID values and many comparisons need to be done based on name, this convertIdsToNames() utility method is frequently used in ValueScripts in the standard reports.

- **Using a QueryScript**: used to specify any custom filter and add it into the queryOptions object that is used in the datasource filter; parameters using a QueryScript do not need to specify a property because the queryScript overrides any property on the parameter; the argument specified on the parameter can be accessed within the script through the “value” variable

  Group and populations are stored in groupDefinitions objects as a filter, so this example (from the Identity Forwarding Report) shows how a group or population selected as a report parameter is built into the datasource filter through a QueryScript.

  ```
  <Parameter argument="groupDefinitions">
     <QueryScript>
        <Source>
           import sailpoint.object.*;
           import sailpoint.reporting.*;
           Filter f = ReportingLibrary.getGroupDefinitionFilter(context, value,
  false);
           if (f!=null) {
              queryOptions.addFilter(f);
           }
           return queryOptions;
        </Source>
     </QueryScript>
  </Parameter>
  ```

- **ValueRule and QueryRule**: These two can be specified in place of ValueScript and QueryScript, respectively, to encapsulate the beanshell of a script into a reusable rule. (These two examples were not pulled from a standard report; they represent the appropriate syntax if the reports using the ValueScript and QueryScript specified above had encapsulated those scripts into rules.)

```
<Parameter argument="applications" property="parent.application">
   <ValueRule>
```

```
      <Reference class="sailpoint.object.Rule" id="4028460238ed9b8e0138ed9beff9090f" name-
e="App Value Rule"/>
   </ValueRule>
</Parameter>

<Parameter argument="groupDefinitions">
   <QueryRule>
      <Reference class="sailpoint.object.Rule" id="4028460238ed9b8e0138ed9beff90900" name-
e="Group Query Rule"/>
   </QueryRule>
</Parameter>
```

Query

Another way to specify the filter contents is though a <Query> element. The contents of Query element are specified as a filter string and can only specify hard-coded criteria with no variable substitution (i.e. report arguments cannot be specified within a Query element). Query allows the specification of “or” criteria, as shown in the example below:

```
<Query>IdentityEntitlement.name=="assignedRoles" || Iden-
tityEntitlement.name=="detectedRoles"</Query>
```

Query and QueryParameters can be specified for the same DataSource. When both are specified, the Query filter and the Parameter filters are “anded” together to create the final where clause.

QueryScript

QueryScript creates a filter string through a beanshell script. It is designed so it can append additional criteria, including those requiring variable substitution, onto a Query element's contents. The script has access to the string value of the Query element (in a string variable called “query”) and must explicitly append the additional criteria to it; otherwise, the original query string is overwritten with the QueryScript's return value. The QueryScript shown below actually comes from an HQL datasource report (the Account Group Membership Totals Report), but the QueryScript syntax is the same for all datasource types.

```
<QueryScript>
   <Source>
      import java.util.*;

      List applications = args.get("application.id");
      if (applications != null &amp;amp;&amp;amp; !applications.isEmpty()){
         query = query + " and application.id in(:application_id) ";
      }
      return query;

    </Source>
</QueryScript>
```

Join

When the search must access more than one object to process the filter criteria, a <Join> element is required to connect the objects properly. One or more Joins can be specified for a single datasource.

For example, the Identity Roles Report displays the roles that each Identity is assigned. Most of the available filters for the report apply to the Identity object, but the role assignment is recorded on the IdentityEntitlement object, linked to the Identity object by the Identity ID. The Join element specifies that connection. The property is the value on the

primary object (the DataSource objectType) and the joinProperty specifies the connection attribute on the second object.

```
<DataSource objectType="Identity" type="Filter">
   <Join joinProperty="IdentityEntitlement.identity.id" property="id"/>
   <Query>IdentityEntitlement.name=="assignedRoles" || Iden-
tityEntitlement.name=="detectedRoles"</Query>
   <QueryParameters>
      <Parameter argument="identities" property="id"/>
      …
   </QueryParameters>
</DataSource>
```

OptionsRule or OptionsScript

The final elements available on a filter datasource are an OptionsRule or OptionsScript. These can be used to make modifications to the QueryOptions before the query is run; they can also replace the rest of the query specification (for example, eliminating the need for a Query, QueryParameters, QueryScript or Join element) by simply constructing the whole queryOptions in the rule or script.

Only one of these can be specified (the rule overrides the script if both are provided). The OptionsRule or OptionsScript is passed a SailPoint Context called “context”, a queryOptions called “options” and an argument map called “args”. Options contains the entire set of query criteria specified in any of the other elements (Query, QueryScript, QueryParameters, Join) and args contains the TaskDefinition argument map. The rule or script should append any additional custom queryOptions to options and return it.

```
<OptionsScript>
    <Source>
       import java.util.*;
       import sailpoint.object.*;
       //code to add components to queryOptions goes here. e.g.: this would
       // Apply to an Identity objectType and would get only Identities whose
       // Manager is the Identity selected in the manager filter (typically,
       // an optionsScript or optionsRule would be used for a more complex
       Filter myFilter = Filter.eq("manager.id", args.get("manager.id");
       options.addFilter(myFilter);
       return options;
     </Source>
 </OptionsScript>
```

An OptionsRule is specified as a reference to a Rule object:

```
<OptionsRule>

    <Reference class="sailpoint.object.Rule" id="4028460238ed9b8e0138ed9beff90900"
name="MyReport Options Rule"/></OptionsRule>
```

Java DataSource

A Java datasource is the next most commonly used report datasource type. The XML to specify this is fairly simple and straightforward; the java class it calls can be as simple or as complex as is required to generate the desired report contents.

The java datasource class must implement the **sailpoint.reporting.datasource.JavaDataSource** interface, as described in the IdentityIQ javadocs. This interface defines all the methods that must be coded. All attributes in the taskDefinition attribute map (including all input attributes from the Signature) are passed to the Java class in an arguments map.

The <DataSource> element in the XML specifies these attributes:

DataSource Attribute	Usage
dataSourceClass	The fully qualified java class name
objectType	The primary object against which searches are performed in the java code
type	Java (tells the report executor this is a Java Datasource)
defaultSort	Optional field; sorts the returned data by the named field if no sort column is specified through the UI or taskDefinition attributes map

> Many of the standard reports were written with a Java Datasource and several examples of this syntax are available. Most of the standard reports use a QueryParameters element to pass data to the DataSource, which allowed the report writer to take advantage of the reportHelper class in the reporting architecture to reuse existing code. However, this is not strictly necessary and isnot commonly done in the field. Because the entire taskDefinition attributes map, including all input attributes from the <Signature>) is passed to the java class in an arguments map, they do not need to be specified as QueryParameters. The class can build the QueryOptions object needed to retrieve the data without passing the values through QueryParameters.

HQL DataSource

An HQL datasource is used in rare circumstances but is available for implementers who need to execute queries that hit Hibernate directly. This should only be used when the report developer is very knowledgeable about HQL. The HQL query must be custom written by the report developer.

Like the Filter datasource, the HQL datasource can specify its query using these types of nested elements: Query, QueryScript, and QueryParameters. The Query and QueryParameters elements function somewhat differently in an HQL datasource, though, so it is important to understand the way they are processed.

The Account Group Membership Totals Report provides an example of an HQL datasource.

```
<LiveReport title="Account Group Membership Totals Report">
   <DataSource type="Hql">
      <Query>from ManagedAttribute m where group=true</Query>
      <QueryParameters>
          <Parameter argument="application" property="application_id"/>
      </QueryParameters>
      <QueryScript>
         <Source>
            import java.util.*;

            List applications = args.get("application.id");
```

```
            if (applications != null &amp;amp;&amp;amp; !applications.isEmpty()){
               query = query + " and application.id in(:application_id) ";
            }
            return query;

          </Source>
      </QueryScript>
   </DataSource>
   <Columns>
        <ReportColumnConfig field="accountGroupName" header="rept_app_account_grp_memb_
col_name" property="value" sortable="true"/>
        <ReportColumnConfig field="accountGroupDisplayName" header="rept_app_account_grp_
display_name" property="displayName" sortable="true"/>
        <ReportColumnConfig field="application" header="rept_app_account_grp_memb_app"
property="application.name" sortable="true"/>
        <ReportColumnConfig field="total" header="rept_app_account_grp_memb_col_members"
property="(select count(*) from IdentityEntitlement ie where ie.value = m.value and ie.ap-
plication = m.application and ie.name = m.attribute and ie.aggregationState = &apos;Con-
nected&apos;)"/>
   </Columns>
</LiveReport>
```

In an HQL datasource, the <Query> element must specify the From clause for the query. The objectType is not required for an HQL datasource and is ignored if it is provided.

Query

The Query element can also specify some or all of the where clause. As on a Filter DataSource, the Query element can specify any hard-coded attribute evaluations (i.e. no variable substitution available) and multiple conditions can be specified with “and” or “or” relationships.

```
<Query>from ManagedAttribute m where group=true</Query>
```

QueryScript

The HQL DataSource <QueryScript> element works just like the Filter Datasource QueryScript. It contains beanshell that returns a filter string (appending to the Query's string and returning the combined string value). However, the difference in QueryParameter processing changes the way variables are processed in the script. The queryScript has access to the task argument map (in its “args” variable), so conditional processing can be done on those arguments in determining how to build the filter string. However, the contents of those variables do not need to be built into the actual query string in the queryScript; they can be referenced as variable names that are passed to the search through QueryParameters. In an HQL datasource, the search is performed based on the query string built in the query and queryScript elements; the parameters specified as QueryParameters are passed to the search method along with that query string and are substituted into the query where variable names are found.

In the example below (from the Account Group Membership Totals Report), the QueryScript examines the application.id value from the args list and if it is non-null, it appends “and application.id in (:application_id) “ to the query string. The QueryParameter application_id allows the list of applications from the task argument list to be substituted for the :application_id variable in that query string when the search is executed.

```
<QueryParameters>
    <Parameter argument="application" property="application_id"/>
</QueryParameters>
<QueryScript>
    <Source>
       import java.util.*;

       List applications = args.get("application.id");
       if (applications != null &amp;amp;&amp;amp; !applications.isEmpty()){
          // :application_id
          query = query + " and application.id in(:application_id) ";
       }
       return query;

    </Source>
</QueryScript>
```

QueryParameters

As explained in the QueryScript section above, the QueryParameters in an HQL datasource do not make up filter components in their own right but instead provide variables for substitution into the query string at the time the search is executed.

The Parameter elements within the QueryParameters for an HQL datasource is usually only specified with an argument and a property. The property is the variable name used in the query string and the argument is the argument map key in which the value to be used in the search is stored. A defaultValue or a valueScript (as described in the Filter datasource's QueryParameters section) can also be used to provide the value for the property, if desired. The Parameter's QueryScript option (which returns a QueryOptions object) cannot be used for an HQL datasource, as it does not provide a value for substitution; HQL datasources do not use a QueryOptions object in their searches.

ReportColumnConfigs

Just as with the other report types, the ReportColumnConfigs within the report's <Columns> element specify the attributes to retrieve from the query for display in the report detail grid - the “Select” portion of the query. The property attributes name the fields to retrieve. The final ReportColumnConfig - the “total” column - in the Account Group Membership Totals Report shows an example of how to include a sub query in the HQL select clause. This provides additional levels of flexibility in reflecting data on the report. A calculated field like this cannot be marked as sortable.

```
<ReportColumnConfig field="total" header="rept_app_account_grp_memb_col_members" prop-
erty="(select count(*) from IdentityEntitlement ie where ie.value = m.value and ie.ap-
plication = m.application and ie.name = m.attribute and ie.aggregationState =
&amp;apos;Connected&amp;apos;)"/>
```

Columns/ReportColumnConfig: Report Grid Presentation

The <ReportColumnConfig> elements within the <Columns> element specify which values should be returned from the query and also define how those values are presented in the report grid.

```
<Columns>
<ReportColumnConfig field="username" header="rept_uncorrelated_ids_grid_username" prop-
erty="nativeIdentity" sortable="true" />
```

```
<ReportColumnConfig field="firstName" header="rept_uncorrelated_ids_grid_firstName" prop-
erty="identity.firstname" sortable="true" />

<ReportColumnConfig field="lastName" header="rept_uncorrelated_ids_grid_lastName" prop-
erty="identity.lastname" sortable="true" />

<ReportColumnConfig field="applicationName" header="rept_uncorrelated_ids_grid_appName"
property="application.name" sortable="true" />
 </Columns>
```

Attributes of ReportColumnConfig include:

Attribute	Usage
field	Unique name for the report column in this report
header	Column label to use in the report body; can be a string or a localizable message key
property	Object property from which the data is pulled; this value is used in the query specification
sortable	Boolean value indicating whether the report body should be sortable by this column; determines whether the column is selectable in the Sort By and Group By fields in the report specification and whether the report can be sorted by this column in preview mode
hidden	Boolean value indicating whether the column should be omitted from the report grid by default. Columns marked as hidden (hidden=”true”) appear in the left-side of the Columns list on the report template's Report Layout page, which makes them available for inclusion. However, by default they are not included on the report. Any report instances that were configured to display these fields in the report grid override this hidden attribute by including the column name in their reportColumnOrder attribute, causing the column to appear in the report output regardless of this attribute's value.
ifEmpty	Optional property to use if the value of the object property is null or empty;See Entitlement Owner Access Review Live Report's accountName field for an example: `<ReportColumnConfig field="accountName" header="rept_data_owner_col_account_name" ifEmpty-y="exceptionEntitlements.nativeIdentity" prop-erty="exceptionEntitlements.displayName" sortable="true" width="110"/>`
subQueryKey	Used for multi-valued properties to show the values as a list of comma-separated values instead of multiple rows in the report. Specifying a subQueryKey automatically renders the column as a subquery that selects the property from the dataSource objectType matching on the subsQueryKey attribute.An example exists in the Manager Access Review Live Report's tags field:

Attribute	Usage
	<ReportColumnConfig field="tags" header="rept_cert_col_tags" property="parent.certification.tags.name" subQueryKey="id" width="110"/>
sortExpression	A set of fields by which the data should be sorted instead of sorting by the selected column. This attribute allows a column that is not sortable to sort the data by columns related to the selected column. See the following example of the permission column on the Account Group Permissions Access Review Live Report. <ReportColumnConfig field="permissions" header="rept_cert_col_account_group_permission" property="exceptionEntitlements"sortExpression="exceptionApplication,exceptionPermissionTarget,exceptionPermissionRight" sortable="true" width="110"> <RenderScript> <Source> return sailpoint.api.EntitlementDescriber.summarize(value); </Source> </RenderScript> </ReportColumnConfig>
scriptArguments	A CSV list of additional properties to pass to a column's RenderScript; see the status field from the Policy Violation Report for an example. The renderScript then accesses these values through its scriptArgs variable (as shown in this example). <ReportColumnConfig field="status" header="rept_viol_grid_col_status" property="status" scriptArguments="identity,policyName,constraintName,created" sortable="true" width="110"> <RenderScript> <Source> import sailpoint.object.*; … String identityId = scriptArgs.get("identity").id; …

Attribute	Usage
	</Source> </RenderScript>
valueClass	Defines the class for the property so it can be displayed appropriately; omitted for string values
skipLocalization	Indicate that the column contains reserved words that should not be translated. Examples include Names or Account names that could contain reserved keywords.

In the standard reports, the only time the “hidden” attribute is used on a ReportColumnConfig is when the column is added to the available set by an ExtendedColumnScript or ExtendedColumnRule (as described in Extended Column Script or Rule). Generally, if a column is relevant to a report, it is displayed on the report by default, though it can be removed from the detail grid by a user if they do not wish to see that data on their customized version of the report.

> Strings and Java constants specified in ReportColumnConfig attributes are evaluated first as message keys for automatic localization; if they do not match a defined message key, the given string value is used.

RenderScript and RenderRule

If the value returned from the query needs to be manipulated into a more user-friendly format for display on the report, this can be accomplished with a RenderScript or RenderRule. A RenderRule is used to encapsulate the beanshell into a reusable rule - useful when the same manipulation might apply to several reports. A RenderScript specifies the beanshell inline within a <Source> element. The column's property attribute is passed into the script in the variable “value”.

This example RenderScript (taken from the Revocation Live Report) displays a different localized message key depending on whether the action.remediationCompleted flag is true or false so that the report column shows an easier-to-interpret “Status” instead of a True/False flag.

```
<ReportColumnConfig field="status" header="rept_remediation_progress_grid_col_status"
property="action.remediationCompleted" sortable="true" width="110">
   <RenderScript>

      <Source>

         import sailpoint.tools.Message;

         import sailpoint.web.messages.MessageKeys;

         return value == true ? Message.localize(MessageKeys.WORK_ITEM_STATE_FINISHED) :
Message.localize(MessageKeys.WORK_ITEM_STATE_OPEN);

     </Source>

         </RenderScript>
</ReportColumnConfig>
```

A RenderRule would be specified like this:

Rendered columns are sorted by the property attribute, not by the displayed value, so the order of rows might not appear alphabetical by the display value. At a minimum, sorting by the column groups all of the rows with the same column value together. Some properties might not be sortable, such as a property that is an object. These columns should be marked as sortable="false" even though the displayed value might seem sortable. Alternatively, a sortExpression can be specified to drive data sorting for these columns.

```
<ReportColumnConfig field="status" header="rept_remediation_progress_grid_col_status"
property="action.remediationCompleted" sortable="true" width="110">
   <RenderRule>
      <Reference class="sailpoint.object.Rule" id="4028460238ed9b8e0138ed9bf61300de" name-
e="Status Message RenderRule"/>
   </RenderRule>
</ReportColumnConfig>
```

Initialization Script or Rule

The initialization script and rule allow the report developer to customize a report to address an installation's unique reporting requirements. These scripts/rules are fairly open-ended and should generally be considered tools for expert-level report creation.

Most often, initialization scripts and rules are used to customize the forms presented to the user for filter specification. For example, several standard reports use an initialization rule to build dynamic forms to present all of the installation's configured Identity attributes - both standard and extended - as filter options on some forms. Another form customization usage might be to change the set of filters available based on other filter selections; for example, a report might present a “privileged” account filter option only when the application selected for the “Application” filter has privileged accounts.

An InitializationScript is specified inline within a <Source> element:

```
<InitializationScript>
   <Source>
     import sailpoint.object.*;
     import sailpoint.reporting.ReportingLibrary;
     … (initialization code goes here; see rule example below)
   </Source></InitializationScript>
```

An InitializationRule is specified as a rule reference with the code encapsulated in the named rule:

```
<InitializationRule>
    <Reference class="sailpoint.object.Rule" id="4028460238ed9b8e0138ed9bf6130000" name-
e="Identity Report Form Customizer"/>
</InitializationRule>
```

The rule shown below is used in several of the standard reports (such as the User Detail Report and Identity Roles Report) to customize a form based on the standard and extended Identity attributes configured for the installation. Similar rules exist to create custom forms for other reports.

```
<Rule language="beanshell" type="ReportCustomizer" name="Identity Report Form Cus-
```

```
tomizer">
 <Description>
    This rule populates a form with fields for the standard and extended identity attrib-
utes.
  </Description>
  <Signature returnType="Map">
    <Inputs>
      <Argument name="locale">
        <Description>
          The current user's locale
        </Description>
      </Argument>
      <Argument name="report">
        <Description>
          The base report
        </Description>
      </Argument>
    </Inputs>
    <Returns>

    </Returns>
  </Signature>
  <Source>
     <![CDATA[
     import sailpoint.object.*;
     import sailpoint.reporting.ReportingLibrary;

     ObjectConfig identityConfig = ObjectConfig.getObjectConfig(Identity.class);
     // Add standard attributes to the form

     List standardAttributes = new ArrayList();
     standardAttributes.add(identityConfig.getObjectAttributeMap().get("firstname"));
     standardAttributes.add(identityConfig.getObjectAttributeMap().get("lastname"));
     standardAttributes.add(identityConfig.getObjectAttributeMap().get("displayName"));
     standardAttributes.add(identityConfig.getObjectAttributeMap().get("email"));
     standardAttributes.add(identityConfig.getObjectAttributeMap().get("manager"));
     standardAttributes.add(identityConfig.getObjectAttributeMap().get("inactive"));

     ReportingLibrary.addAttributes(context, report, Identity.class, standardAttributes,
null, "Identity Attributes", locale);

     // add extended attributes to the form (multi-valued and regular)

     List extendedAttrs = new ArrayList();
     for(ObjectAttribute att : identityConfig.getSearchableAttributes()){
       if (!att.isStandard())
         extendedAttrs.add(att);
     }

     for(ObjectAttribute att : identityConfig.getMultiAttributeList()){
         extendedAttrs.add(att);
     }

     ReportingLibrary.addAttributes(context, report, Identity.class, extendedAttrs, null,
"Identity Extended Attributes", locale);
```

```
    ]]>
</Source>
</Rule>
```

The methods in the ReportingLibrary (like the one used in this example rule) are documented in the IdentityIQ Javadocs. The addAttributes method, for example, does the following:

1. Determines the form page where the attributes should be displayed (selects by section name, creates a new page based on the section name if not found, or selects the first page after Standard Properties if no section is specified)
2. Adds each attribute as an extended argument to the LiveReport object
3. Adds each attribute to the datasource QueryParameters list as a Parameter
4. Defines a Field object for each attribute and adds it to the Section

These methods can be used in custom report development, but note that it is possible that they could change in future versions of IdentityIQ, requiring those reports that rely on them to be revisited and modified. Alternatively, the code to add the attributes to the query parameters and form fields list can be explicitly written by the datasource developer.

> When an initialization script/rule is in place, if any of the functionality depends on the value of a specific form field, that field must be specified with the postBack attribute set to true (postBack= "true"); this causes the form to submit and reload when that value changes, and causes the initialization rule or script to execute again, picking up the new value for the field.

Signature Extended Arguments

When the initialization script or rule adds new fields to a report form, the values must be saved for any report instance for which they were specified, and they must be passed to the report at runtime to be used as report filters. This is done by adding them as extended arguments in the report definition; from there, they are automatically stored in the report instance's argument map when the report instance's TaskDefinition is saved. Even though these arguments do not exist in the report template's signature, they are generated at runtime by the initialization script and the values from the template's argument map are applied for the report's execution.

> This only works for these initialization-generated attributes; all static form fields must be explicitly specified in the report template's signature for them to be used in the report generation. Attributes that are included in the report instance's attribute map that do not exist in the report signature and are not generated by the initialization script or rule is not applied to the report as filters at runtime.

Extended Column Script or Rule

An extended column script or rule can be used to add additional columns to a form based on other attributes selected. For example, the script shown below adds application-attribute columns to the set of available columns based on the application selected on the form (for example, if an application has a “privileged” or “service” account attribute, these can be optionally included in the report output when that application is selected as a filter for the report while they would not be available if a different application that did not have these attributes were selected). The extendedColumnScript or Rule should return a list of ReportColumnConfig objects; these are automatically added to the Columns list as “hidden” columns - available for inclusion on the report but not included in the report detail grid by default.

This script comes from the User Account Attributes Report and is used to add columns to the report output based on which application is selected as a filter for the report.

```
<ExtendedColumnScript>
   <Source>

   import java.util.*;
   import sailpoint.reporting.*;
   import sailpoint.object.*;

   List newCols = new ArrayList();
   Map formValues = form.getFieldValues();
   if (formValues != null &amp;&amp; formValues.containsKey("application") &amp;&amp;
formValues.get("application") != null){
       newCols = ReportingLibrary.createApplicationAttributeColumns(context, formVal-
ues.get("application"));
   }

   return newCols;

   </Source>
</ExtendedColumnScript>
An ExtendedColumnRule is specified as a rule reference with the code encapsulated in the
named rule:
<ExtendedColumnRule>
    <Reference class="sailpoint.object.Rule" id="4028460238ed9b8e0138ed9bf6130000" name-
e="Application Extended Column Rule"/>
</ExtendedColumnRule>
```

> When an extended column script/rule is in place, the field on which its functionality depends must be specified with the postBack attribute set to true (postBack= "true"); this causes the form to submit and reload when that filter field's data value changes, causing the ExtendedColumnRule to fire and detect the required condition for displaying the columns.

When columns are added to the report as a result of this rule, they first appear as “hidden” columns - available for inclusion in the report output but not selected for it. While they are still hidden, they are not saved in the report instance's XML but are regenerated as hidden columns by this rule every time the report specification is edited. Once the user adds the columns to the report detail's column list, the columns are saved in the customized report instance's attributes map in the ReportColumnOrder element, prefixed with the associated application's ID; if the report is later edited to reference a different application, these columns are automatically deleted from the report.

Validation Script or Rule

A validation rule or script is used to validate the data entered on a report form. For example, if a value is required for a specific filter for the report to run, that field can be validated as being non-null by a ValidationRule or ValidationScript.

A Validation script contains the code inline, wrapped in a <Source> element.

```
<ValidationScript>
    <Source>
        import java.util.*;
```

```
        import sailpoint.reporting.*;
        import sailpoint.object.*;
        List messages = new ArrayList();
        … (validation code goes here - see rule example below)
        return messages;
    </Source>
</ValidationScript>
```

A validation Rule is called by reference:

```
<ValidationRule>
    <Reference class="sailpoint.object.Rule" id="4028460238ed9b8e0138ed9bf61300ff" name-
e="Privileged Access Report Validation Rule"/>
</ValidationRule>
```

This validation rule checks the field on the Privileged Account Attributes form for a null (or empty) value; the report requires that a value be specified for this field, so an error message is displayed and the report does not run if this field does not pass this validation. A validation script or rule returns a list of messages; if the form passes validation, this list should be empty.

```
<Rule language="beanshell" type="ReportValidator" name="Privileged Access Report Val-
idation Rule">
   <Description>
      This rule validates the Privileged Access Report Form
    </Description>
    <Signature returnType="java.util.List">
      <Inputs>
        <Argument name="context">
          <Description>
            A sailpoint.api.SailPointContext object that can be used to query the data-
base if necessary.
          </Description>
        </Argument>
        <Argument name="report">
          <Description>
            The report object
          </Description>
        </Argument>
        <Argument name="form">
          <Description>
            The submitted sailpoint Form object.
          </Description>
        </Argument>
      </Inputs>
      <Returns>
        <Argument name="messages">
          <Description>
            A list of error messages.
          </Description>
        </Argument>
```

```
      </Returns>
    </Signature>
    <Source>
      <![CDATA[
       import java.util.*;
       import sailpoint.object.*;
       import sailpoint.tools.Message;
       List messages = new ArrayList();

       Form.Section section = form.getSection("Priviledged Account Attributes");
       boolean found = false;
       for(FormItem item : section.getItems()){
         Field field = (Field)item;
         if(field.getValue() != null && field.getValue() != "") {
           found = true;
         }
       }

       if (!found)
            messages.add(Message.localize("rept_priv_access_err_no_attr"));

       return messages;
      ]]>
  </Source>
</Rule>
```

ReportSummary: Summary Table

The <ReportSummary> element describes the summary table in the summary section of the report.

The table header is specified in the title attribute.

```
<ReportSummary title="Uncorrelated Account Details">
```

The report summary has its own datasource; it does not use the same datasource as the report detail grid. The datasource for the report summary can be specified as a script or a rule. A script is most commonly used, but the datasource beanshell can be encapsulated in a rule for reusability if desired. Both are expressed as nested elements (<DataSourceScript> or <DataSourceRule>).

The DataSourceScript or DataSourceRule for the ReportSummary is passed these parameters:

DataSourceScript or Rule Parameters	Contents/Purpose
Context	A SailPoint Context object for executing the search
reportArgs	The TaskDefinition argument/attribute map
Report	The entire LiveReport report definition
baseHql	The from and where clause used in the report detail search if the report

DataSourceScript or Rule Parameters	Contents/Purpose
	DataSource was an HQL datasource; null if DataSource type was not HQL
baseQueryOptions	The QueryOptions (specifying the “where” clause criteria) used in the report detail search if the report DataSource was a Filter datasource; null if Datasource type was not Filter

The summary table is usually built from data retrieved through one or more database queries that are specified and executed by the script or rule through the context (SailPointContext object), passing it a QueryOptions object populated with the necessary Filter objects. The example here illustrates how this is done.

```
<ReportSummary title="Uncorrelated Account Details">
    <DataSourceScript>
       <Source>

          import java.util.*;
          import sailpoint.tools.Util;
          import java.lang.Math;
          import sailpoint.object.*;
          import sailpoint.api.ObjectUtil;

          QueryOptions ops = new QueryOptions();
          ops.addGroupBy("correlated");

          String sources = "";
          // retrieve list of apps in reportArgs argument map; add IDs to
          // filter and names to CSV list to display as summary's "Sources" value
          if (reportArgs.containsKey("correlatedApps")){
             List apps = reportArgs.getList("correlatedApps");
             if (apps != null){
                ops.addFilter(Filter.in("links.application.id", apps));
                List appNames = ObjectUtil.convertIdsToNames(context, Application.class,
apps);
                sources = Util.listToCsv(appNames);
             }
          }

          List fields = new ArrayList();
          fields.add("correlated");
          fields.add("count(*)");

          int correlated = 0;
          int uncorrelated = 0;

          // get counts per Identity with links on the named applications,
          // subdivided by "correlated" flag
          Iterator results = context.search(Identity.class, ops, fields);
          while(results.hasNext()){
             Object[] row = results.next();
             int count = Util.otoi(row[1]);
```

```
            // add counts to correlated or uncorrelated totals based on correlated
            // flag
            if ((Boolean)row[0]){
               correlated += count;
            } else {
               uncorrelated += count;
            }
         }
         // calculate percentage of accounts that are correlated
         float percent =  correlated != 0 ? (float)uncorrelated/correlated : 0;
         String percentString = ((int)Math.floor(percent * 100)) +  "%";

         // add values to hashmap; these name/value pairs are displayed in the
         // report summary through the XML's LiveReportSummaryValue elements
         Map map = new HashMap();
         map.put("sources", sources);
         map.put("correlatedIdentities", correlated);
         map.put("uncorrelatedIdentities", uncorrelated);
         map.put("totalIdentities", correlated + uncorrelated);
         map.put("percentCorrelated", percentString);

         return map;

      </Source>
   </DataSourceScript>
```

A datasource rule would be specified as a nested element (<DataSourceRule>) that contains a rule reference.

```
<DataSourceRule>
<Reference class="sailpoint.object.Rule" id="4028460238ed9b8e0138ed9beff9090f" name-
e="UncorrelatedAcct Report Summary Rule"/>
</DataSourceRule>
```

The datasource script or rule returns a hashMap of values that are used to populate the corresponding LiveReportSummaryValue elements (based on their name attributes) in the ReportSummary's Values list. The LiveReportSummaryValue elements each include a unique name and a label attribute. The label can be specified as a string or a localizable message key and is displayed alongside the value in the Report's summary section.`<ReportSummary title="Uncorrelated Account Details">`

```
   <DataSourceScript>
      <Source>
         …
         Map map = new HashMap();
         map.put("sources", sources);
         map.put("correlatedIdentities", correlated);
         map.put("uncorrelatedIdentities", uncorrelated);
         map.put("totalIdentities", correlated + uncorrelated);
```

```
          map.put("percentCorrelated", percentString);

          return map;
       </Source>
    </DataSourceScript>
    <Values>
       <LiveReportSummaryValue label="rept_uncorrelated_ids_grid_label_auth_sources" name-
e="sources"/>
       <LiveReportSummaryValue label="rept_uncorrelated_ids_summary_correlated" name-
e="correlatedIdentities"/>
       <LiveReportSummaryValue label="rept_uncorrelated_ids_summary_uncorrelated" name-
e="uncorrelatedIdentities"/>
       <LiveReportSummaryValue label="rept_uncorrelated_ids_summary_total_ids" name-
e="totalIdentities"/>
       <LiveReportSummaryValue label="rept_uncorrelated_ids_summary_percent" name-
e="percentCorrelated"/>
    </Values>
</ReportSummary>
```

Chart: Report Graph

The Chart element defines the graph that is displayed in the Summary section of the report. The chart can be represented as a pie chart or as a column or line graph. The chart data is based on the dataset for the report detail grid (the DataSource element) unless a DataSourceRule or Script is specified for the chart. Commonly, the chart represents the report body's data, grouped and counted by groupings (i.e. “value” is a count, grouped by the category and/or series).

Attributes available to define the chart are listed in this table:

Attribute	Usage
title	Name to display above the chart
type	Identifies the type of chart to display (pie, column, or line)
category	Defines the X axis in line or column graphs; defines the separate sections of a pie graph
value	Defines the Y axis in line or column graphs; defines the portion (fraction) of the pie that belongs to each section in a pie graph; often a count
series	Defines the separate columns or lines on line or column graphs; ignored for pie charts
groupBy	String value of column name (or CSV list of column names) to group data by for graphing counts
sortBy	List of sort columns for data; seldom used since groupBy can specify multiple fields in a CSV list
limit	Limits the number of records examined for the graph; seldom used, unless a similar limit was imposed on the report detail data, because the graph should generally represent all of the data in the report detail

Attribute	Usage
script	Used to define a datasource for the chart other than the report detail data; script contains a <Source> element with BeanShell content
dataSourceRule	Used to define a datasource for the chart other than the report details data; contains a reference to a rule where the BeanShell has been encapsulated
nullSeries	Label to display if the series value (x-axis) is null (for example, a null certification action status means "Open" so that should be the label for the group of certifications whose action.status is null)
nullCategory	Label to display for data group when the category value is null

In most cases, the chart is created by selecting the value, category, and series fields from the object queried by the report detail datasource using the exact same filter criteria used by that datasource. The table below describes how the chart data is retrieved by default (when a dataSourceRule or Script are not specified for the chart).

Report Detail DataSource Type	Default Chart Query
Filter	DataSource's objectType object is queried using the queryOptions built from the DataSource Query, QueryScript, and QueryParameters elements
Java	Requires the DataSource class to have implemented the getBaseQueryOptions method; this method should return the QueryOptions used in the report detail query; also requires that the objectType is specified on the DataSource; retrieves the data for the chart from the objectType object using the QueryOptions returned by getBaseQueryOptions()
HQL	Uses the same query string employed by the report detail query, which specifies both the From and the Where clauses, to retrieve the chart's data

Standard Chart Examples

This example pie chart from the Uncorrelated Accounts Report examines the uncorrelated account data pulled from Links, groups it by application.id and counts the number of uncorrelated accounts on each application. The graph represents the number of uncorrelated accounts from each application (in this case, one uncorrelated account was found per application).

```
<Chart category="application.name" groupBy="application.id" title="rept_uncorrelated_ids_
chart_title" type="pie" value="count(*)"/>
```

The Manager Access Review Report contains an example of a Column graph that shows the count of certification items that are open, approved, or revoked (reflected in the action.status attribute), separated by roles and additional entitlements if applicable (reflected in the type attribute).

```
<Chart category="type" groupBy="action.status,type" nullSeries="cert_action_open" series-
s="action.status" title="rept_cert_chart_title" type="column" value="count(*)"/>
```

Chart Script and DataSourceRule

The script and dataSourceRule elements can provide the report writer more flexibility in creating charts based on any data. However, these are generally used only in rare cases in custom reports. The standard reports do not use a Script or DataSourceRule for their charts.

When either of these is used, the BeanShell within them is provided the following parameters:

DataSourceRule or Script Parameters	Contents/Purpose
context	A SailPoint Context for executing the search
args	The TaskDefinition Arguments map
report	The entire LiveReport report definition
baseHql	The from and where clause used in the report detail search if the report DataSource was an HQL datasource; null if DataSource type was not HQL
baseQueryOptions	The QueryOptions (specifying the “where” clause criteria) used in the report detail search if the report DataSource was a Filter datasource; null if Datasource type was not Filter

The code must return a list of maps (List<Map<String, Object>>) with each map representing the value, category, and series for each component of the chart. If there is no series, the “series” should be recorded as empty string ("") rather than null.

For example:

```
{[("value","23"), ("category","ADAM"),("series","")],
[("value","5"), ("category","Financials"),("series","")],
[("value","12"), ("category","PeopleSoft"),("series","")]}
```

The rule or script can add onto the existing criteria from the report detail's DataSource by modifying the baseHql or baseQueryOptions or it can build the chart data with completely independent criteria. The BeanShell is responsible for specifying the desired columns and search criteria, executing the database search to retrieve the data, formatting the data into the list of maps, and returning that list.

Report Forms

The layouts and contents of report-specific form pages are specified within a Form object, referenced by the report XML in a <ReportForm> element, nested within the <LiveReport> report definition. The Form object must be created and imported into IdentityIQ separately and is referenced by name.

Each <Section> defines a separate page on the Edit Report window. The page name, shown in the Sections list and at the top of the form, is specified as the Section's label attribute.

```
   <Form name="Uncorrelated Accounts Report Custom Fields">
      <Section label="Uncorrelated Accounts Parameters" name="customProperties">
<Field displayName="report_input_correlated_apps" filterString="logical==false &amp;&amp;
authoritative==false" helpKey="rept_input_uncorrelated_ident_report_correlated_apps" name-
e="correlatedApps" type="Application" value="ref:correlatedApps"/>
      </Section>
    </Form>
```

Reports with large numbers of available parameters often include multiple report-specific-parameter pages, specified as multiple Sections in the Form XML, to group the parameters by category.

```
 <Form name="Identity Report Options Form Skeleton">
    <Section columns="2" label="rept_priv_access_section_priv_account_attrs" name-
e="Priviledged Account Attributes">
       <Attributes>
          <Map>
            <entry key="subtitle" value="rept_priv_access_section_instructions"/>
          </Map>
       </Attributes>
     </Section>
    <Section columns="2" label="rept_priv_access_section_account_props" name="Account
Properties">
        <Field columnSpan="1" displayName="rept_identity_roles_field_app" helpKey="rept_
identity_roles_helpN_app" multi="true" name="applications" type="Application" value-
e="ref:applications"/>
    </Section>
    <Section columns="2" label="rept_priv_access_section_identity_props" name="Identity
Properties"/>
    <Section columns="2" label="rept_priv_access_section_identity_extended_props" name-
e="Identity Extended Properties"/>
</Form>
```

> Several of the sections in this example XML do not contain any Field definitions. This is because this report uses an initialization rule to create the form fields for those sections based on system data. See Initialization Script or Rule for more information on these dynamic forms.

These are the attributes that can be specified for the Section element.

Section Attribute	Usage
label	The label for the form; can be a string or a localizable message key
name	Name for the section; must be unique per form; used programmatically but not displayed on the UI Edit Report window
Columns	Used to specify the number of columns in which fields should be displayed; fields are displayed in the order they are listed within the section, with one field added to each

Section Attribute	Usage
	column in a repeating pattern; for example, in a 2-column layout, 5 fields would be displayed like this: Field 1 Field 2 Field 3 Field 4 Field 5 This attribute can be omitted for a one-column display.

Fields on each form are specified as nested <Field> elements within each <Section>. Important report-form attributes on the Field element are described below.

```
Field displayName="report_input_correlated_apps"

filterString="logical==false &amp;&amp; authoritative==false" helpKey="rept_input_uncor-
related_ident_report_correlated_apps" name="correlatedApps" type="Application" value-
e="ref:correlatedApps"/>
```

Field Attribute	Usage
displayName	The label for the field. Can be a string or a localizable message key.
helpKey	The tool tip for the field. Can be a string or a localizable message key.
name	Name for the field and must be unique per form.
type	Field type. If this entry is an object, it is automatically created as a suggest, allowing the user to select from the system's existing objects of that type.
filterString	A filter string that restricts the set of objects presented to the user for selection. Only applies to objects that are presented as suggest boxes.
value	A reference to the XML input parameter from which to retrieve the starting / default value for the field. This is how the saved values in customized report instances are populated on the form when those instances are viewed in the Edit Report window. Input parameters to the TaskDefinition XML are specified in its signature, as described in Report Signature: Passing Data from Saved Report Instances below.
postBack	A flag indicating if the form should be submitted when the field value changes.This causes the form to be reloaded and any initialization actions to be performed. This flag is important if an initializationScript or Rule or an ExtendedColumnScript or Rule needs to run to add or remove fields on the form or columns on the report based on this field value.

Field Attribute	Usage

AllowedValuesDefinition	This is specified as a nested element to provide a list of values from which the form user can select. See the User Activity Report for an example (excerpted below).
	
	`<Field columnSpan="1" displayName="label_action" helpKey="rept_input_app_activity_report_action" multi="true" name="action" type="string" value-e="ref:action">`
	`<AllowedValuesDefinition>`
	`<Script>`
	`<Source>`
	`import sailpoint.object.*;`
	
	`List items = new ArrayList();`
	`for(ApplicationActivity.Action action : Applic-ationActivity.Action.values()) {`
	`List l2 = new ArrayList();`
	`l2.add(action.toString());`
	`l2.add(action.getMessageKey());`
	`items.add(l2);`
	`}`
	`return items;`
	`</Source>`
	`</Script>`
	`</AllowedValuesDefinition>`

Custom report forms are presented to users in the Edit Report window, along with the Standard Properties page and the Report Layout page. The Standard Properties and Report Layout pages are standard components of the report architecture and are automatically presented for any standard or custom report that implements the LiveReport architecture, whether or not the report references a custom form for report-specific parameters. The Standard Properties page is always presented first and the Report Layout page is always last; report-specific form pages are inserted between these two on the Edit Report window.

Reports DataSource Example

The following sample report uses a Java data source. This sample displays Identities' name, display name, and manager status and can be filtered by the manager to whom the Identities report and applications on which the Identities have accounts. Both of these filters are multi-selectable.

Java data source example:

```
<TaskDefinition name="Sample Report" executor="sailpoint.reporting.LiveReportExecutor"
  subType="Identity Reports" resultAction="Rename"
  progressMode="Percentage" template="true" type="LiveReport">
   <Description>Sample report</Description>
   <RequiredRights>
       <Reference class="sailpoint.object.SPRight"
         name="FullAccessBusinessRoleMembershipReport"/>
   </RequiredRights>
   <Attributes>
      <Map>
        <entry key="report">
           <value>
             <LiveReport title="Manager Status Report">
               <DataSource type="Java"
                 dataSourceClass="sailpoint.reporting.datasource.SampleDataSource"
                 defaultSort="name">
                  <QueryParameters>
                   <Parameter argument="applications"
                     property="links.application.id"/>
                   <Parameter argument="managers" property="manager.id"/>
                  </QueryParameters>
               </DataSource>
               <Columns>
                 <ReportColumnConfig field="name" header="Identity Name" property="name"
sortable="true"/>
                 <ReportColumnConfig field="displayName" header="Display Name" sort-
able="true"/>
                 <ReportColumnConfig field="managerStatus" header="Is Manager" prop-
erty="managerStatus" sortable="true"/>
               </Columns>
             </LiveReport>
           </value>
        </entry>
      </Map>
   </Attributes>
   <Signature>
       <Inputs>
          <Argument multi="true" name="applications" type="Application"/>
          <Argument multi="true" name="managers" type="Identity"/>
       </Inputs>
   </Signature>
</TaskDefinition>
```

This Java datasource builds and runs the query for this report based on the filters the user specifies.

SampleDataSource.java

```
/* (c) Copyright 2012 SailPoint Technologies, Inc., All Rights Reserved. */
package sailpoint.reporting.datasource;

import net.sf.jasperreports.engine.JRException;
import net.sf.jasperreports.engine.JRField;
import sailpoint.api.sailpointContext;
import sailpoint.object.Attributes;
import sailpoint.object.Filter;
import sailpoint.object.Identity;
import sailpoint.object.LiveReport;
import sailpoint.object.QueryOptions;
import sailpoint.object.Sort;
import sailpoint.task.Monitor;
import sailpoint.tools.GeneralException;
import sailpoint.tools.Util;

import java.util.Arrays;
import java.util.Iterator;
import java.util.List;

public class SampleDataSource implements JavaDataSource {

    private Monitor monitor;

    private sailpointContext context;
    private QueryOptions baseQueryOptions;
    private Integer startRow;
    private Integer pageSize;

    private Object[] currentRow;
    private Iterator<Object[]> iterator;

    public void initialize(sailpointContext context, LiveReport report, Attrib-
utes<String, Object> arguments, String groupBy, List<Sort> sort) throws GeneralException
{
        this.context = context;

        baseQueryOptions = new QueryOptions();

        if (arguments.containsKey("applications")){
            List<String> applicationIds = arguments.getList("applications");
            baseQueryOptions.add(Filter.in("links.application.id", applicationIds));
        }

        if (arguments.containsKey("managers")){
            List<String> managersIds = arguments.getList("managers");
            baseQueryOptions.add(Filter.in("manager.id", managersIds));
        }

        if (sort != null){
            for(Sort sortItem : sort) {
                baseQueryOptions.addOrdering(sortItem.getField(), sortItem.isAscending
());
            }
        }
```

```
        if (groupBy != null)
            baseQueryOptions.setGroupBys(Arrays.asList(groupBy));
    }

    private void prepare() throws GeneralException{
        QueryOptions ops = new QueryOptions(baseQueryOptions);

        if (startRow != null && startRow > 0){
            ops.setFirstRow(startRow);
        }

        if (pageSize != null && pageSize > 0){
            ops.setResultLimit(pageSize);
        }

        iterator = context.search(Identity.class, ops, Arrays.asList("name", "dis-
playName", "managerStatus"));
    }

    public boolean next() throws JRException {

        if (iterator == null){
            try {
                prepare();
            } catch (GeneralException e) {
                throw new JRException(e);
            }
        }

        if (iterator.hasNext()){
            currentRow = iterator.next();
            return true;
        }

        return false;
    }

    public Object getFieldValue(String field) throws GeneralException {
        if ("name".equals(field)){
            return currentRow[0];
        } else if ("displayName".equals(field)){
            return currentRow[1];
        } else if ("managerStatus".equals(field)){
            return currentRow[2];
        } else {
            throw new GeneralException("Unknown column '"+field+"'");
        }
    }

    public void setLimit(int startRow, int pageSize) {
        this.startRow = startRow;
        this.pageSize = pageSize;
    }
```

```
    public int getSizeEstimate() throws GeneralException {
        return context.countObjects(Identity.class, baseQueryOptions);
    }

    public void close() {

    }

    public Object getFieldValue(JRField jrField) throws JRException {
        String name = jrField.getName();
        try {
            return getFieldValue(name);
        } catch (GeneralException e) {
            throw new JRException(e);
        }
    }

    public void setMonitor(Monitor monitor) {
        this.monitor = monitor;
    }

    public QueryOptions getBaseQueryOptions() {
        return baseQueryOptions;
    }

    /**
     * Unused since this is not an hql report.
     */
    public String getBaseHql() {
        return null;
    }
}
```